

ESX Switch Administrator's Guide



Copyright " 1998 FORE Systems, Inc. All rights reserved.

U.S. Government Restricted Rights. If you are licensing the Software on behalf of the U.S. Government ("Government"), the following provisions apply to you. If the Software is supplied to the Department of Defense ("DoD"), it is classified as "Commercial Computer Software" under paragraph 252.227-7014 of the DoD Supplement to the Federal Acquisition Regulations ("DFARS") (or any successor regulations) and the Government is acquiring only the license rights granted herein (the license rights customarily provided to non-Government users). If the Software is supplied to any unit or agency of the Government other than DoD, it is classified as "Restricted Computer Software" and the Government's rights in the Software are defined in paragraph 52.227-19 of the Federal Acquisition Regulations ("FAR") (or any successor regulations) or, in the cases of NASA, in paragraph 18.52.227-86 of the NASA Supplement to the FAR (or any successor regulations).

ESX is a trademark of FORE Systems, Inc.

NT is a registered trademark of Microsoft Corporation.

FireWall-1 is a registered trademark of Check PointTM Software Technologies Inc.

In the U.S.A., you can contact FORE Systems' Technical Support using any one of the following methods:

- You can receive online support via TACTics Online at: <http://www.fore.com>
- You can contact Technical Support via e-mail at: support@fore.com
- You can telephone your questions to Technical Support at: 1-800-671-FORE (3673) or +1 724-742-6999
- You can FAX your questions to Technical Support at: +1 724-742-7900

Technical support for non-U.S.A. customers should be handled through your local distributor.

No matter which method is used for support, please be prepared to provide your support contract ID number, the serial number(s) of the product(s), and as much information as possible describing your problem/question.

IMPORTANT

CAREFULLY READ THE FOLLOWING TERMS, CONDITIONS AND RESTRICTIONS BEFORE INSTALLATION AND USE OF ANY SOFTWARE PROGRAMS PROVIDED BY FORE SYSTEMS, INCORPORATED. OPENING THE SEALED

SOFTWARE PACKAGE AND/OR INSTALLATION OR USE OF SUCH SOFTWARE PROGRAMS SHALL BE DEEMED ACCEPTANCE OF THESE TERMS, CONDITIONS AND RESTRICTIONS.

IF YOU DO NOT AGREE WITH AND ACCEPT THESE TERMS, CONDITIONS AND RESTRICTIONS, PROMPTLY RETURN ALL SUCH SOFTWARE AND HARDWARE PRODUCTS TO FORE SYSTEMS, INC. AND ANY FEES PAID FOR SUCH PRODUCTS WILL BE REFUNDED.

1. LICENSE

Subject to the terms and restrictions set forth in this License, FORE Systems, Inc. ("FORE") grants a non-exclusive non-transferable (except as provided herein) license to use the software programs ("Programs") for use with FORE and/or third party hardware products.

2. COPYRIGHT

The Programs, and all related documentation, are protected by copyright and title to all programs is retained by FORE. You may not copy or otherwise use the Programs, in whole or part, except as expressly permitted in this License. You must reproduce and maintain the copyright notice on any authorized copy you make or use of the Programs.

3. RESTRICTIONS ON USE AND TRANSFER

The Programs may be copied solely for installation and back-up purposes. You may not modify the Programs in any manner without the prior written approval of FORE. You may physically transfer the Programs and this License, along with the related FORE hardware, if applicable, to another party only if (i) the other party accepts the terms, conditions and restrictions of this License, (ii) all copies of Programs and related documentation that are not transferred to the other party are destroyed or returned to FORE, (iii) the related FORE hardware for programs designed solely to operate on FORE hardware, is also transferred to the other party, and (iv) you comply with all applicable laws including any import/export control regulations.

4. LIMITED WARRANTY

FORE warrants that the Programs will perform substantially in accordance with the accompanying documentation for a period of ninety (90) days from the date of shipment. This warranty is void if failure is the result of accident, abuse or misuse.

FORE warrants that any media on which the Programs are recorded will be free from defects in materials and workmanship under normal use for a period of ninety (90) days from the date the Programs are delivered to you. If a defect in any such media should occur during this 90-day period, the media may be returned to FORE, at 1000 FORE Drive, Warrendale, Pennsylvania 15086-7502 U.S.A., and FORE will replace the media without charge to you. FORE shall have no responsibility to replace media if the failure of media results from accident, abuse, or misuse.

The program contains third party software which is not fault-tolerant and is not designed, manufactured or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the program could lead directly to death, personal injury, or severe physical or environmental damage ("High Risk Activities"). Accordingly, FORE and FORE's third party licensors specifically disclaim any express or implied warranty of fitness for High Risk Activities.

EXCEPT FOR THE WARRANTIES SPECIFICALLY STATED IN THIS ARTICLE, FORE HEREBY DISCLAIMS ALL EXPRESS OR IMPLIED WARRANTIES OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you. This limited warranty gives you specific legal rights, and you may also have other rights which vary from jurisdiction to jurisdiction.

5. LIMITATION OF LIABILITY

Your exclusive remedy and the entire liability of FORE related to the Programs shall be, at FORE's option: (i) refund of the price paid for the Programs, (ii) correction of the Programs so they perform as warranted, or in the case of media failure, replacement of media as provided above. In no event will FORE or anyone else who has been involved in the creation, production, or delivery of the Programs be liable for any damages, including, without limitation, direct, incidental or consequential damages, loss of anticipated profits or benefits, resulting from the use of the Programs, even if FORE has been advised of the possibility of such damages.

6. TERM

This License is effective until terminated. You may terminate this License at any time by destroying all copies of the Programs and related documentation. This License will terminate automatically if you fail to comply with any term or condition of this License, including any attempt to transfer a copy of the Programs to another party except as provided in this License. You agree that, upon such termination, you will destroy all copies of the Programs and related documentation.

7. CONFIDENTIALITY

You agree that the source code applicable to the Programs is confidential and proprietary to FORE. Accordingly, you may not decompile, reverse engineer or otherwise manipulate the Programs so as to derive such source code.

8. U.S. GOVERNMENT RESTRICTED RIGHTS LEGEND

If you are licensing the Software on behalf of the U.S. Government ("Government"), the following provisions apply. If the Software is supplied to the Department of Defense ("DoD"), it is classified as "Commercial Computer Software" under paragraph 252.227-7014 of the DoD Supplement to the Federal Acquisition Regulations ("DFARS") (or any successor regulations) and the Government is acquiring only the license rights granted herein (the license rights customarily provided to non-Government users). If the Software is supplied to any unit or agency of the Government other than DoD, it is classified as "Restricted Computer Software" and the Government's rights in the Software are defined in paragraph 52.227-19 of the Federal Acquisition Regulations ("FAR") (or any successor regulations) or, in the case of NASA, in paragraph 18.52.227-86 of the NASA Supplement to the FAR (or any successor regulations). Use, duplication or disclosure by the Government is subject to the restrictions set forth in such sections. The Contractor for the Programs is FORE Systems, Inc., 1000 FORE Drive, Warrendale, Pennsylvania 15086-7502.

YOUR USE OF THE PROGRAMS ACKNOWLEDGES THAT YOU HAVE READ THIS END-USER SOFTWARE LICENSE, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS, CONDITIONS AND RESTRICTIONS. YOU FURTHER AGREE THAT THIS LICENSE IS THE COMPLETE AND EXCLUSIVE STATEMENT OF YOUR AGREEMENT WITH FORE AND SUPERSEDES ANY PROPOSAL OR PRIOR AGREEMENT, ORAL OR WRITTEN, AND ANY OTHER COMMUNICATIONS RELATING TO THE SUBJECT MATTER OF THIS LICENSE.

FCC Statement

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

Canadian D.O.C

This Class A digital equipment meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

VCCI

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用する
と電波妨害を引き起こすことがあります。この場合には使用者が適切な対策
を講ずるよう要求されることがあります。

VCCI—A**Class 1 Laser Notification**

As the following indicates, our fiber-optic transceivers on the Gigabit media cards meet class 1 laser product standards.



The **ESX Switch Administrator's Guide** provides flowcharts that describe navigation paths. These paths help you access configuration menus and wizards. It also gives procedural steps and examples to show how to configure the system.

Flowchart Shape Represents

In Tree View

Starting point for navigation—often tree view or display view, and occasionally navigation begins with a main configuration page.

Right-Click Chassis Icon

A navigation step:

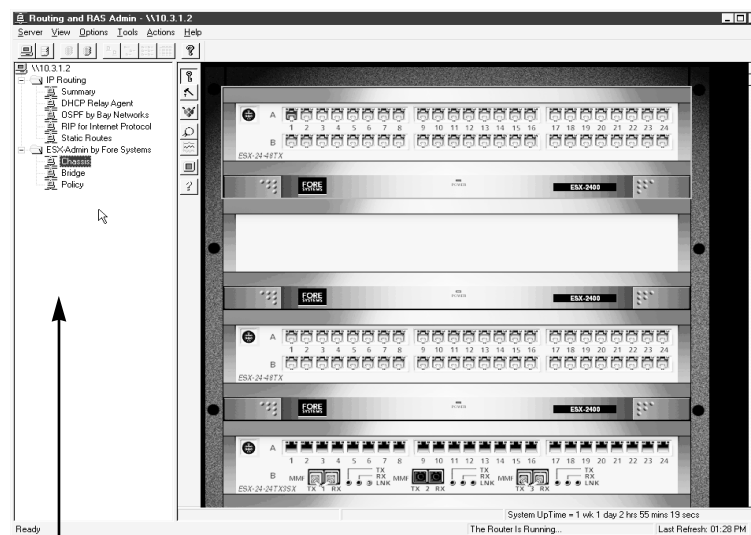
- **Right-click**—displays a pull down menu.
- **Select**—selects an icon or menu item using one of the following techniques:
 - **Left mouse click**—picks a single item..
 - **Drag click**—activates a selection window.
 - **Shift click**—selects contiguous icons.
 - **Control shift click**—selects non-contiguous icons.

Select Configure Chassis

Modify Chassis Configuration Page

A procedure or task

Example: Tree View and Chassis Display



Tree View

Select configuration menus and view status.

Display View

Enter editing mode, select ports, and view system status.

In the previous example, clicking the *chassis* icon, shown in the *tree view*, fills the *display view* with a graphic view of the chassis. Navigation starts by positioning the mouse in either the tree view or in the display view.

To select multiple consecutive ports:








When configuring ports on the switch, you may want to select multiple ports and configure them identically. To select multiple, consecutive ports, press the CTRL key while you hold down the left mouse button activating a lasso, and use the lasso to select multiple consecutive ports.

Accessing Context-sensitive and Topic Online Help

- To access **context sensitive online help**, first click on the ? icon on the **horizontal menu bar** at the top of the screen. When a ? appears next to the mouse pointer, click on an area in a dialog box to display a help message for a field, a control button or area within the dialog box.
- To access **ESX-Admin help topics**, click on the ? icon on the **vertical menu bar** at the top of the screen. An index of help topics will appear on the screen

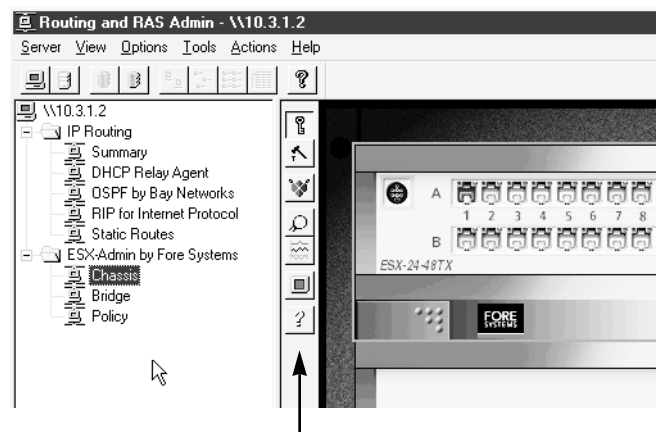
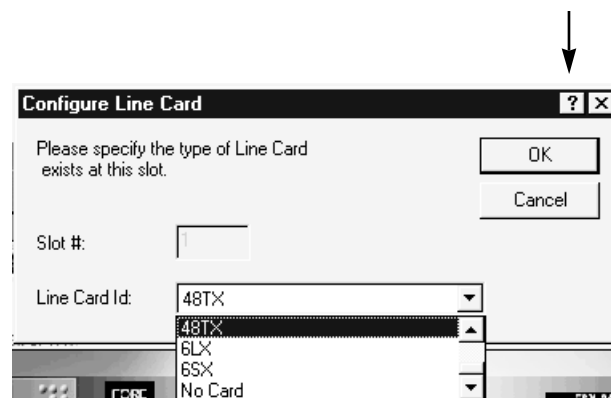
Using Icons to Access ESX-Admin Commands

The *vertical menu bar* contains seven icons, stacked vertically in the border area between the tree view and the display view. By clicking an icon you can access commands directly from the main menu.. A description of menu bar icons and their associated commands follows:

	Edit Mode - toggle edit mode & display edit menu
	Configure - set switch/port parameters
	Edit Policy - configure policies on the switch
	Show Port Info - display port statistics
	ESX-Mon - access the monitoring facility
	Scale Window - expand or shrink the display
	Online Help - view ESX-Admin help topics

Example: Vertical and Horizontal Menu Bars

Horizontal Menu Bar ? Icon- Context-sensitive Online Help



Vertical Menu Bar Icons - Short cut to commands

A Note to the Reader:

This version of the *ESX Switch Administrator's Guide* (Part Number: MANU0387-01) documents Release 4.2 of the ESX-Vision software.

Please provide comments on the documentation to:
support@fore.com

Thanks in advance for providing your comments. Your comments will help us create documentation that will satisfy your information needs.

Chapter 1 Introduction	1-1
1.1 Site Preparation and Equipment Requirements Checklist	1-2
1.2 Installation Tips.....	1-3
Chapter 2 Installing the ESX-4800 Switch	2-1
2.1 Unpack the ESX-4800 Switch	2-2
2.2 Inspect the Shipment	2-3
2.3 Unpack and Install the NSC Enclosure	2-4
2.4 Remove Power Supplies, Fans and Line Cards	2-5
2.5 Install the Chassis in the Rack	2-7
2.6 Unpack and Install the NSC.....	2-8
2.7 Install Power Supplies, Fans and Line Cards	2-9
2.8 Connect a Terminal and Management Station to the NSC.....	2-10
2.9 Connect the NSC to the Switch	2-11
2.10 Power On the Switch Chassis	2-12
2.11 Power On the NSC, Terminals, and Management Station	2-15
2.12 Install the Switch Covers	2-16
Chapter 3 Installing the ESX-2400 Switch.....	3-1
3.1 Unpack the Switch Modules	3-2
3.2 Inspect the Shipment	3-4
3.3 Unpack and Install the Integrated Stack	3-5
3.4 Install a Switch Module in the Stack	3-6
3.5 Install a Switch Module in the Rack	3-8
3.6 Unpack and Install the NSC.....	3-9

3.7 Connect a Terminal and Management Station	3-10
3.8 Connect the NSC to a Switch Module	3-11
3.9 Power On the Integrated Stack	3-12
3.10 Power On a Switch Module Installed in the Rack	3-13
3.11 Power On the Terminal and the NSC	3-14
Chapter 4 Startup	4-1
4.1 System Overview	4-2
4.1.1 Switch Components	4-2
4.1.2 Switch Operating Characteristics	4-2
4.1.3 Control and Management Paths	4-2
4.1.4 Connecting User Equipment to the Switch	4-2
4.2 Startup Sequence	4-4
4.2.1 Startup Sequence Overview	4-4
4.2.2 Startup Procedure	4-5
4.3 Connect Equipment to the Switch	4-8
4.3.1 Identify the Port Connected to the NSC	4-8
4.3.2 Connect User Equipment to Switch Ports	4-9
4.3.3 Establish Compatible Speed and Mode Settings	4-10
4.3.4 Check Port LEDS	4-11
4.4 Start the Management Software	4-13
4.4.1 Load Management Software	4-14
4.4.2 Install the ESX-Vision Software in Your Network Management Station	4-15
4.4.3 Start the ESX-Admin Management Tool	4-16
4.5 Access the Chassis Display	4-17

Chapter 5 Switch Configuration.....5-1

- 5.1 Configuration Overview.....5-2**
- 5.2 Configure Chassis.....5-4**
- 5.3 Configure Line Cards.....5-6**
- 5.4 Configure Ports5-8**
 - 5.4.1 Configure Control Interfaces5-9
 - 5.4.2 Configure Ethernet Interfaces5-10
- 5.5 Cold Standby5-12**
 - 5.5.1 Connecting the Two NSCs to the Switch5-12
 - 5.5.2 Connecting the Two NSCs Together5-12
 - 5.5.3 Configuring the Backup NSC.....5-13
- 5.5 View Port Information5-14**
- 5.6 View Chassis Information.....5-15**

Chapter 6 Configuring Bridging6-1

- 6.1 Bridging Overview.....6-2**
- 6.2 Bridge Creation Wizard6-6**
- 6.3 Create Transparent Bridge Group.....6-7**
- 6.4 Configure Spanning Tree Protocol.....6-9**
- 6.5 Viewing Bridging Information6-11**

Chapter 7 Configuring IP Routing and Protocols.....7-1

- 7.1 Configuring IP Routing7-2**
 - 7.1.1 Assign IP Addresses to Ports7-3
 - 7.1.2 Configure IP Parameters7-6
 - 7.1.3 Configure Interfaces.....7-9
 - 7.1.4 Configure a Static ARP Entry7-13

- 7.1.5 View TCP/IP Information7-15
- 7.1.6 View IP Statistics7-16
- 7.1.7 View ARP Table7-18

7.2 Configuring OSPF7-20

- 7.2.1 Add the OSPF Protocol7-21
- 7.2.2 Define the Router's ID and Type7-22
- 7.2.3 Assign a Router to an Area or Areas7-23
- 7.2.4 Set the Router's Interface Parameters7-24
- 7.2.5 Configure the Border Router's Parameters ..7-32
- 7.2.6 View OSPF Information.....7-42

7.3 Configuring RIP7-47

- 7.3.1 Add the RIP Protocol.....7-48
- 7.3.2 Configure the RIP Protocol7-49
- 7.3.3 Set the Router's Interface Parameters7-52
- 7.3.4 View RIP Information7-58

7.4 Configuring Static Routes.....7-60

- 7.4.1 Add a Static Route to an Interface.....7-61
- 7.4.2 View IP Route Information (IP Routing Table)7-62

7.5 Configuring DHCP7-64**Chapter 8 Configuring Trunking.....8-1**

- 8.1 Trunking Overview.....8-2**
- 8.2 Creating a Trunk Group.....8-4**
- 8.3 Adding Ports to a Trunk Group.....8-5**
- 8.4 Removing Ports from a Trunk Group.....8-6**
- 8.5 Deleting a Trunk Group.....8-7**
- 8.6 Configuring Bridging on a Trunk Group.....8-8**
- 8.7 Configuring IP on a Trunk Group.....8-9**

Chapter 9 Performance Monitoring	9-1
9.1 Performance Monitoring Overview	9-2
9.2 Berkeley Networks Objects and Counters..	9-2
9.3 Starting ESX-Mon	9-2
9.4 Displaying Counters.....	9-4
9.5 Printing a Window Display.....	9-7
9.6 Logging and Viewing Logs	9-8
 Chapter 10 Troubleshooting	 10-1
10.1 Troubleshooting Overview.....	10-2
10.1.1 Switch and Network Configurations	10-2
10.1.2 Problem Solving Checklist.....	10-2
10.2 Troubleshooting Tools.....	10-2
10.2.1 ESX- Commands	10-3
10.2.2 dc Test.....	10-3
10.2.3 NT Troubleshooting Tools	10-6
10.3 Startup and Hardware Problems.....	10-8
10.4 Ethernet Problems.....	10-9
10.5 Bridged Network Problems	10-10
10.6 TCP/IP Problems.....	10-11
10.7 SNMP Problems	10-12
10.8 Managing and Reconstructing Disks	10-13
10.8.1 Detect a Hard drive Failure	10-14
10.8.2 Start Adaptec and Verify a Drive Failure.....	10-15
10.8.3 Rescan a Disk Array.....	10-16
10.8.4 Remove and Replace a Drive	10-17

10.8.5 Reconstruct an Array	10-18
10.8 Reporting Problems	10-20
Chapter 11 Policies	11-1
11.1 Policies Overview	11-2
11.1.1 The Packet Header	11-2
11.1.2 Source and Destination IP Addresses	11-2
11.1.3 Source and Destination Port Numbers	11-2
11.1.4 Determining Whether to Enforce a Policy	11-2
11.1.5 Policy Actions.....	11-2
11.2 Policies and How They Work	11-3
11.2.1 Creating and Enforcing Policies.....	11-3
11.2.2 Actions.....	11-3
11.2.3 Policies and Application Port Numbers	11-3
11.2.4 Global and Specific Policies	11-3
11.3 Creating Application Policies.....	11-4
11.3.1 Access the Application Policy Page	11-4
11.3.2 Name the Application Policy	11-3
11.3.3 Select the Ports for the Policy	11-3
11.3.4 Add an Application to the Policy.....	11-6
11.3.5 Specify the Policy Action.....	11-8
11.4 Adding Ports to a Policy	11-9
11.5 Removing Ports from a Policy	11-10
11.6 Deleting an Application Policy	11-11

The Administrator Guide describes how to administer the ESX-4800 and ESX-2400 switches. It starts with site planning and covers switch installation, startup, and configuration of the switch. It describes bridge, IP, routing protocol, and trunking configuration. It provides information to help you monitor the performance of the switch, and it covers troubleshooting tools and tips to help identify and resolve problems.

Chapter 1	Introduction
Chapter 2	Installing the ESX-4800 Switch
Chapter 3	Installing the ESX-2400 Switch
Chapter 4	Startup
Chapter 5	Switch Configuration
Chapter 6	Configuring Bridging
Chapter 7	Configuring IP Routing and Protocols
Chapter 8	Configuring Trunking
Chapter 9	Performance Monitoring
Chapter 10	Troubleshooting
Chapter 11	Policies

1.1 Site Preparation and Equipment Requirements Checklist

This checklist will help you prepare the site and provide the necessary equipment for installation.

- ☐ A safe, clean, accessible location to install the switch with a minimum of 12 inches of clearance, front and back, for cooling air and for easy access.
- ☐ **Caution:** At the site, maintain a temperature range between 12° and 30° C, and a humidity range between 0% and 90%, non-condensing to avoid damaging the equipment. Where possible, provide a temperature-controlled, air-conditioned area.
- ☐ A standard 19" equipment rack for mounting the switch.
- ☐ Two dedicated power circuits supplying either 110 volt, 20 amp AC or 220 volt, 10 amp AC are recommended for powering the ESX-4800 switch. It will work with one power circuit.
- ☐ One dedicated power circuit supplying either 110 volt, 20 amp AC or 220 volt, 10 amp AC is required for powering the ESX-2400.
- ☐ **Caution:** Attach the ESD-preventative wrist strap supplied with the switch to your wrist and ground it on the cabinet, before attempting to remove or replace a switch modules, fan, or power supply to avoid damaging electronic circuitry.
- ☐ Three Uninterruptible Power Supplies (UPS's) are recommended for powering the ESX-4800 switch: two for the switch chassis and one for the NSC. They provide a continuous supply of current to the system if a brownout or short power outage occurs.
- ☐ Two UPS's are recommended for powering the ESX-2400 switch: one for the switch chassis and one for the NSC.
- ☐ Straight-through cables to connect user equipment to the switch.
 - Cat-5 cables with RJ-45 connectors for 10/100 Base TX connections.
 - 50µ or 62.5µ multi-mode fiber cables with Duplex-SC connectors for 1000 Base SX connections.
 - 9µ single mode fiber cables with Duplex-SC connectors for 1000 Base LX connections.
- ☐ An analog phone jack, phone line, and external modem for performing remote diagnostics.
- ☐ A CD-ROM drive connected to a PC running NT 4.0 that you can use to load the eVision management software, described in Chapter 4.

1.2 Installation Tips

- ☐ Avoid crossing interface cables with power cables where possible to prevent unnecessary interference.
- ☐ Do not place the switch on the floor where dust can accumulate and be drawn into the system by the fans.

Warnings and Cautions

Caution: Use care in lifting and moving heavy objects. Wear an ESD-preventative wrist strap when installing, removing, or replacing components in the cabinet (line cards, power supplies, and fans) to protect electrical circuitry.

Warning

Make sure that the ESX-4800 switch is installed by qualified technicians in an area with restricted access. Technicians must use care in installing and maintaining the switch. The amplitudes and energy levels provided by the switch can produce electric shocks resulting in serious injury or death.

警告

アクセスが制限された個所に、資格のあるサービス係員によって e8 exponeNT Switch がインストールされていることをご確認ください。サービス係員は、インストールとスイッチの補修の際には注意する必要があります。感電によるけがや感電死をもたらす恐れがある、危険な電圧量とエネルギー レベルが存在しています。

Avertissement

Vérifier que le commutateur ESX-4800 est installé par des techniciens compétents sur une zone d'accès réservé. Les techniciens doivent faire attention lors de l'installation et du maintien du commutateur. La tension et les niveaux d'énergie élevés peuvent produire des chocs électriques et occasionner des blessures ou la mort.

Achtung

Installation des ESX-4800 -Schalters nur durch qualifiziertes Wartungspersonal in einem Bereich mit beschränktem Zugang. Vorsicht bei Installation und Wartung des Schalters. Achtung: Hochspannung–Lebensgefahr.

Before installing your system, make sure you've made the necessary preparations and have the necessary equipment. (See the Site Planning Checklist.)

Chapter 2 describes how to install the **ESX-4800** Switch. It consists of the following sections. Together, they contain step-by-step procedures describing how to:

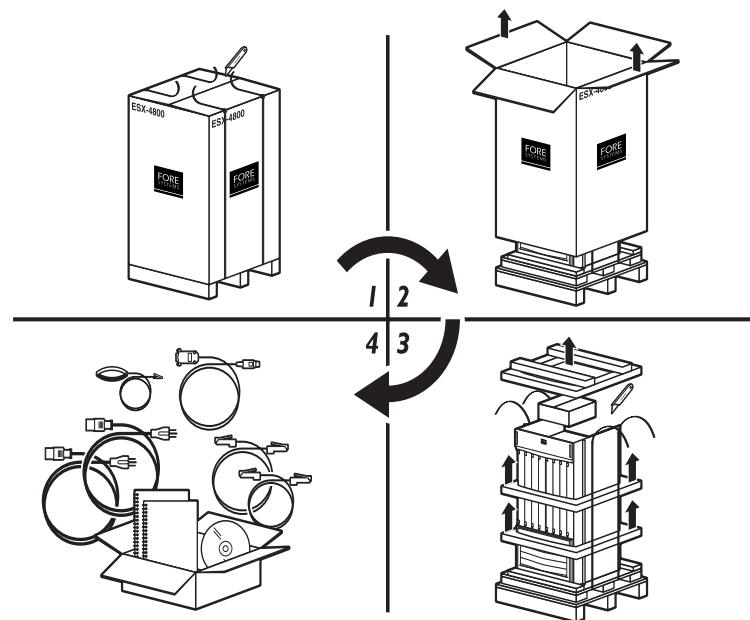
- 2.1 Unpack the **ESX-4800** Switch
- 2.2 Inspect the Shipment
- 2.3 Unpack and Install the NSC Enclosure
- 2.4 Remove Power Supplies, Fans, and Line Cards
- 2.5 Install the Chassis in the Rack
- 2.6 Unpack and Install the NSC
- 2.7 Install Power Supplies, Fans, and Line Cards
- 2.8 Connect a Terminal and Management Station to the NSC
- 2.9 Connect the NSC to the Switch Chassis
- 2.10 Power On the Switch Chassis
- 2.11 Power On the NSC, Terminal, and Management Station
- 2.12 Install the Switch Covers

2.1 Unpack the ESX-4800 Switch

Before unpacking and signing off on the shipment, check the condition of the shipping container and make a note of any damage. Follow these procedures to unpack the switch and the Network Service Controller (NSC).

1. Using a pallet jack, move the pallet-mounted shipping carton containing the switch chassis and the smaller carton containing the NSC close to the rack where you will install the ESX-4800 Switch.
2. Carefully cut the bands securing the shipping carton containing the switch chassis to the shipping pallet.
3. Carefully cut any tape holding the top flaps of the shipping container together.
4. Fold back the flaps on the top of the box.
5. Grab two opposing flaps and lift the box off the switch chassis. The switch chassis will remain strapped to the pallet.
6. Cut the straps securing the switch chassis to the pallet and remove the packing material protecting the top of the switch chassis.

Note: The front cover mounted at the top of the ESX-4800 Switch and the front cover of the NSC may be packed in protective material located on top of the switch chassis. You will install the covers during the last installation step.

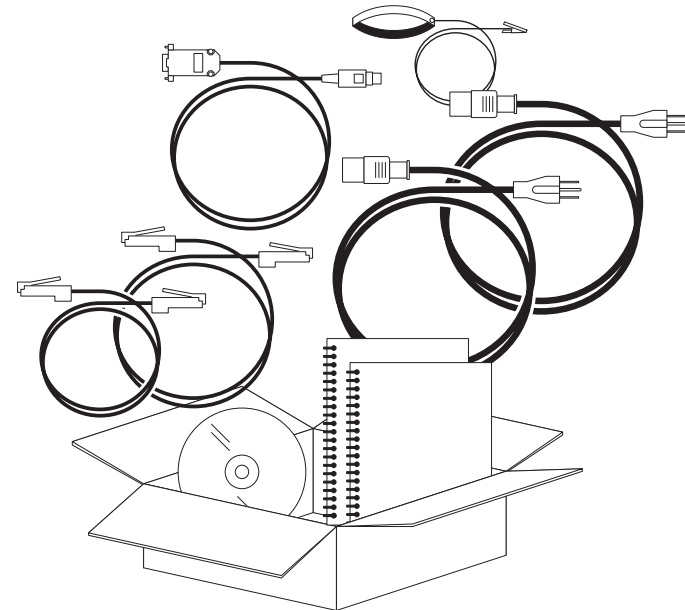


Unpacking the ESX-4800 Switch Chassis

2.2 Inspect the Shipment

While unpacking, check the contents of the shipment:

1. Remove the cardboard box from top of the switch chassis.
2. Open the box carefully and check the contents. The box should contain:
 - 2 Power cords
For powering the switch chassis
 - 2 RJ-45 cables (a short cable and a long cable)
For connecting the switch chassis to the NSC
 - DB-9 serial cable
For connecting a terminal to the NSC's serial port
 - ESD-preventative wrist strap
For protecting electrical circuits from damage due to static discharge
 - CD-ROM
For installing the ESX-Vision management software on a management station connected to the NSC
 - **ESX Switch Administrator's Guide**
For learning to install, startup, and configure the switch using the ESX-Admin GUI management tool
 - **ESX-Cli Command Console Guide**
For learning to use the ESX-Cli command line management tool
3. Make a note of any damage or discrepancy and notify FORE Systems.

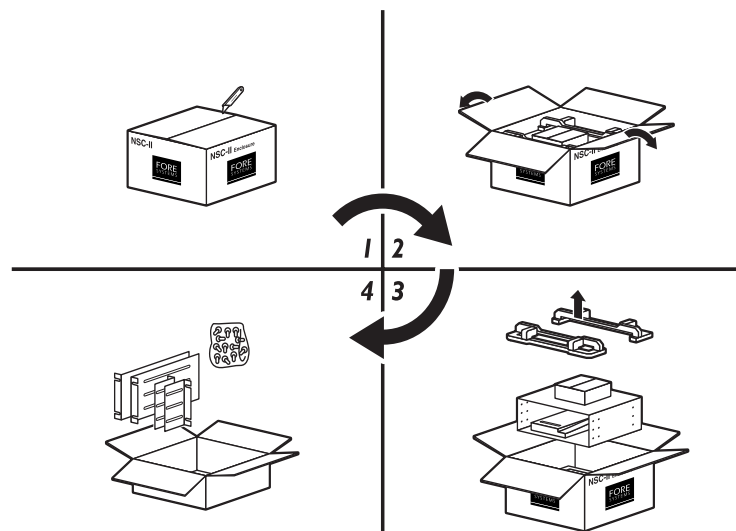


Inspecting the Shipment

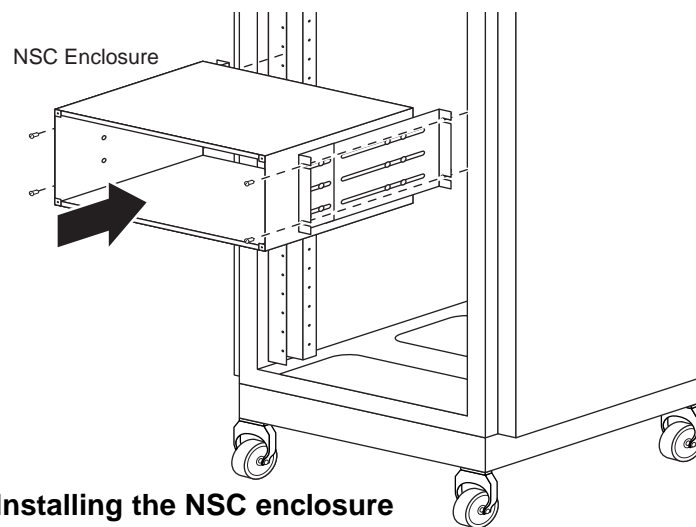
2.3 Unpack and Install the NSC Enclosure

Once installed in the rack, the NSC Enclosure provides a secure shelf on which to place the chassis while aligning the holes in the chassis with those in the rack. Before installing the NSC Enclosure, follow these instructions to unpack it:

1. Carefully cut the tape holding the top flaps of the shipping carton together.
2. Fold back the flaps on the top of the box.
3. Remove the packing materials from the top of the box, and remove the accessory box containing a power cord and screws you will use to attach the NSC brackets to the NSC.
4. Remove the NSC Enclosure from the shipping carton, and remove the NSC brackets from inside the NSC enclosure.
5. Attach both sliding brackets to the outside of the back of the NSC enclosure, loosely, with the screws that are provided.
6. Tilt the NSC enclosure, slide it into the rack, making sure that the brackets extend beyond the vertical stands of the rack and rest it on the bottom of the rack.
7. Lift the NSC enclosure vertically, and while keeping it level, align the mounting holes located on both sides of the enclosure, front and back, with the mounting holes in the rack.
8. While one person holds the NSC in position, a second person can attach the NSC enclosure brackets to the rack, with machine screws.



Unpacking the NSC enclosure



Installing the NSC enclosure

2.4 Remove Power Supplies, Fans, and Line Cards

We recommend that you lighten the weight of the chassis by removing the power supplies, fans, and line cards before installing it in the rack.

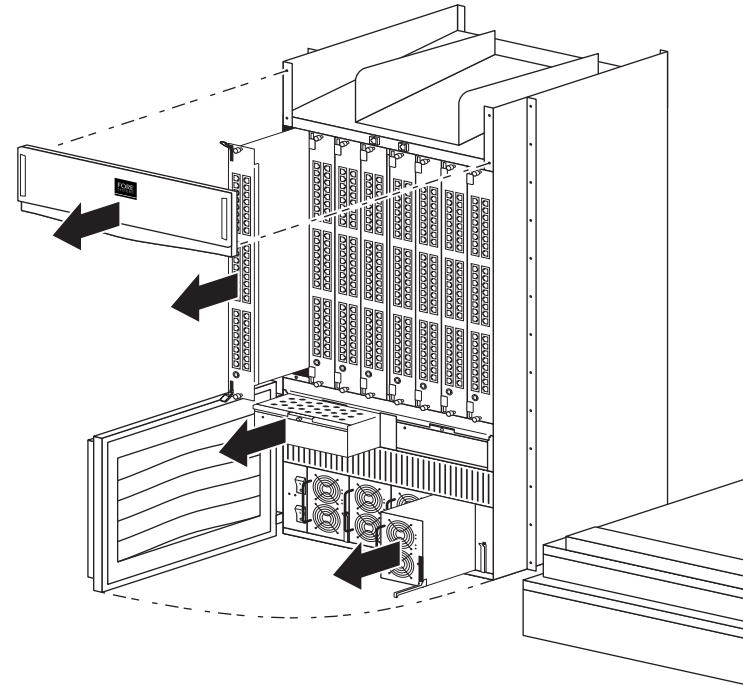
Carefully lift the chassis off the pallet, taking care not to damage the chassis or the components when placing it on the floor.

Caution: We recommend that you use at least two technicians to lift the chassis off the pallet and follow safe lifting practices to avoid back strain and injury.

Note: The front cover mounted at the top of the ESX-4800 Switch and the front cover of the NSC may be packed in protective material located on top of the switch chassis. You will install the covers during the last installation step.

Before removing components as shown in the detailed drawings on the following page, perform the following steps:

1. Remove the cover from the top of the chassis.
If the cover does not pull off easily, carefully insert a flat bladed screwdriver between at each corner of the chassis and the cover prying gently until the cover loosens.
Note: Skip this step if the switch chassis was shipped with the front cover removed. The cover may have been packed at the top of the switch chassis.
2. Open the door covering the fans and power supplies as shown in the illustration.



Removing Power Supplies, Fans, and Line Cards

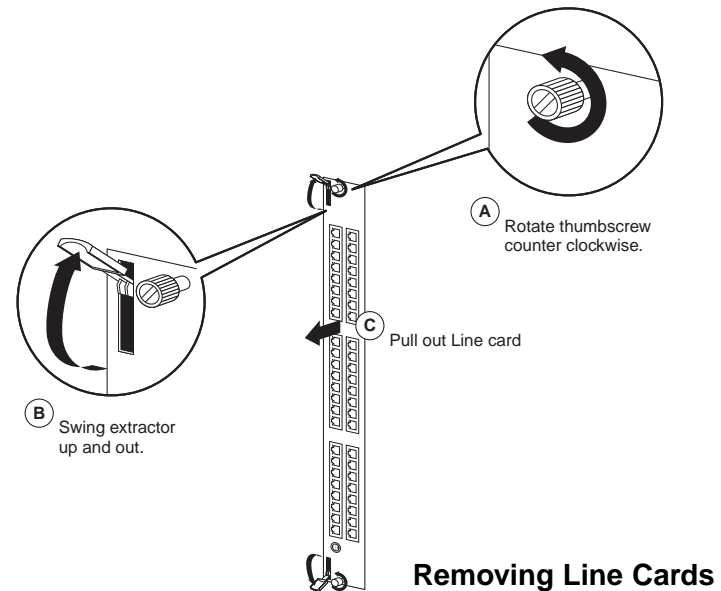
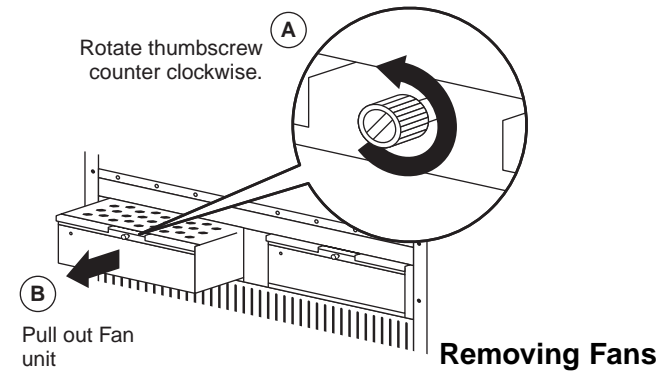
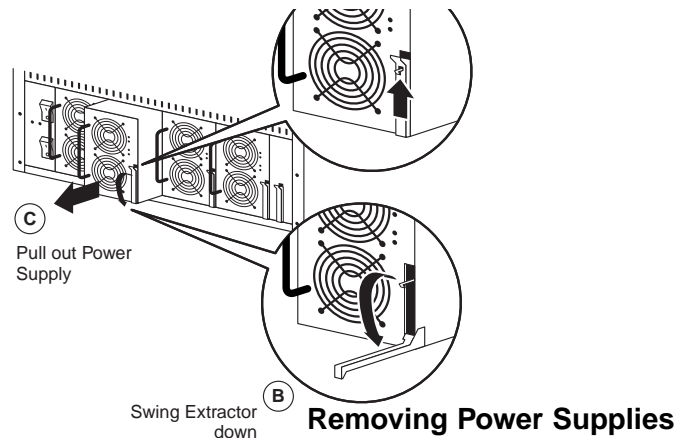
2.4 Remove Power Supplies, Fans, and Line Cards (continued)

Before installing the ESX-4800 Switch in the rack, remove the power supplies, fan units, and line cards from the switch chassis to lighten the weight of the chassis before installing it in the rack.

Caution: Because the modular components contain integrated circuits, make sure that you use an ESD grounding strap before removing or replacing them. After removal, place the modular components on a safe, clean, non-metallic surface where they will be protected from damage, including ESD.

Follow the instructions in the illustrations to remove:

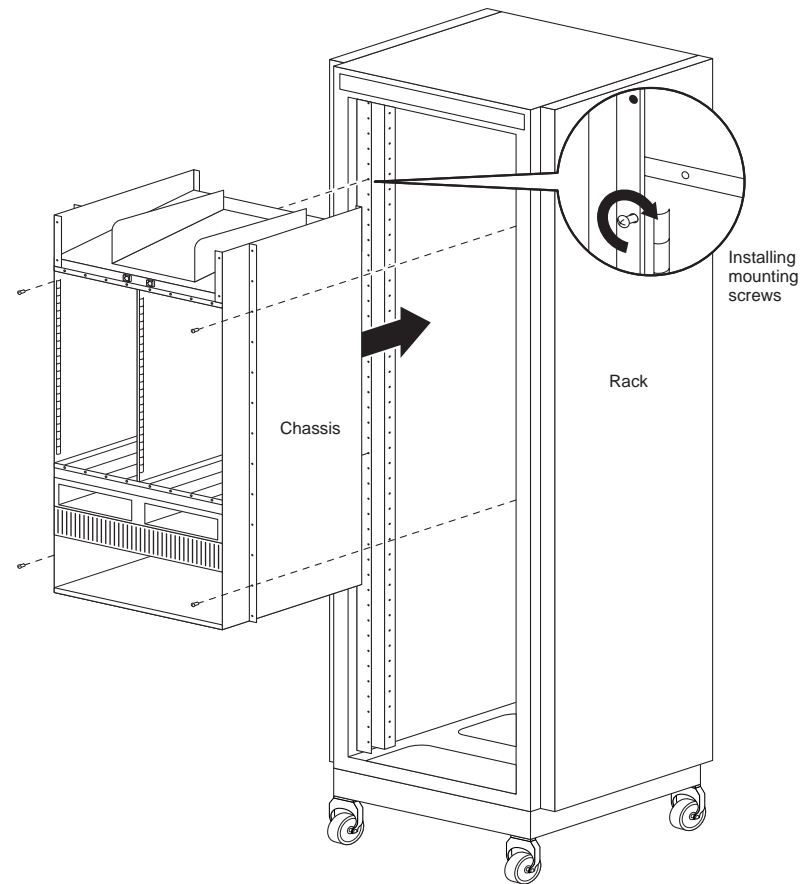
- Power Supplies
- Fan Units
- Line Cards



2.5 Install the Chassis in the Rack

After removing the modular components, install the switch chassis in the rack.

1. Lift the switch chassis and position it in the rack on top of the NSC enclosure.
2. Align the mounting holes and secure the switch chassis in the rack with machine screws that meet the thread requirements of the holes in your rack.

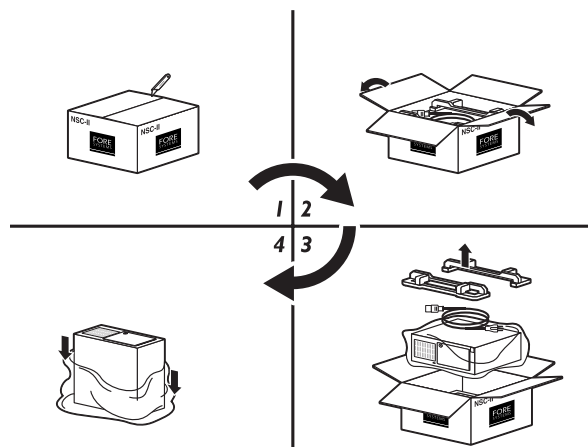


Installing the Chassis

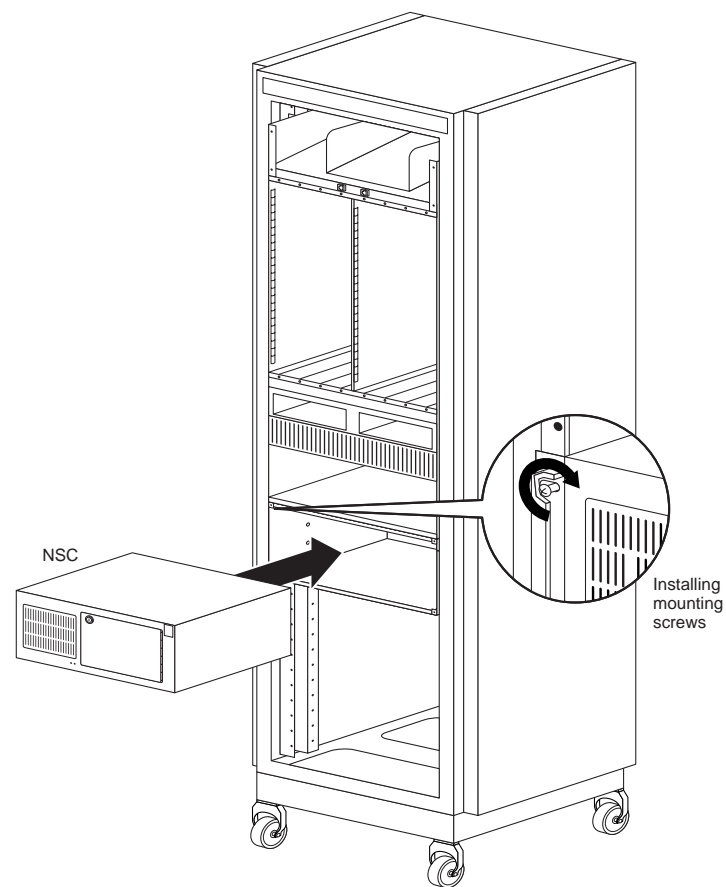
2.6 Unpack and Install the NSC

Follow these instructions to unpack and install the NSC:

1. Carefully cut the tape holding the top flaps of the shipping carton together.
2. Fold back the flaps on the top of the box.
3. Remove packing materials and the power cord from the top of the box.
4. Remove the NSC from the shipping carton, remove the poly bag from the NSC, and place it inside the NSC Enclosure.



Unpacking the NSC

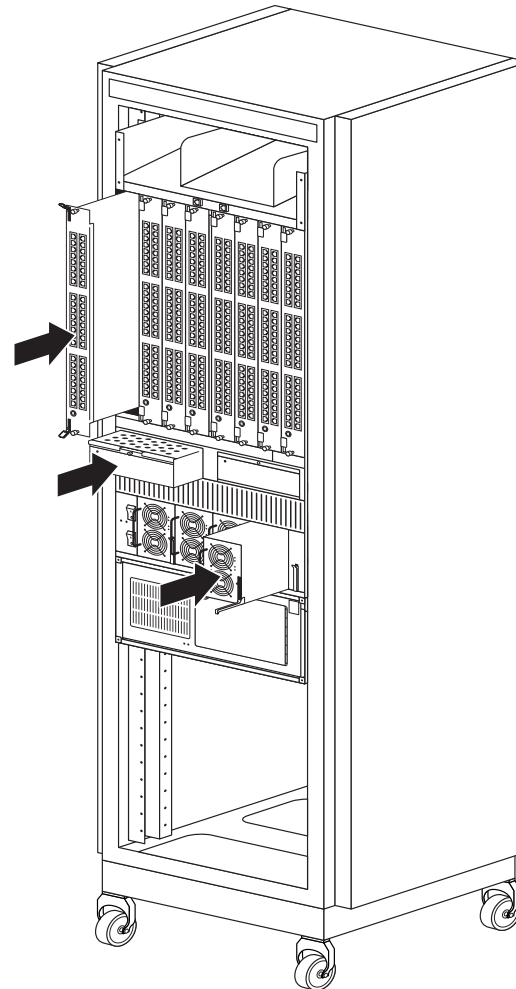


Installing the NSC

2.7 Install Power Supplies, Fans, and Line Cards

The illustration on this page shows how to install the line cards, fans, and power supplies in the chassis. For more detailed instructions, refer to the illustrations in Section 2.5 that show how to remove these components, and reverse the steps.

Note: Locate the bar-coded, numbered label on the front of the chassis. When you configure the switch, you will enter that number in the software.



**Installing Power Supplies,
Fans, and Line Cards**

2.8 Connect a Terminal and a Management Station to the NSC

After mounting the chassis and the NSC in the rack, follow these instructions to connect a terminal and management station to the NSC. You can use a single device as both a management station and a terminal:

1. Connect a terminal to the NSC's Com 1 serial port using a DB9 null modem cable—required to startup the system. (See Section 4, Startup.)

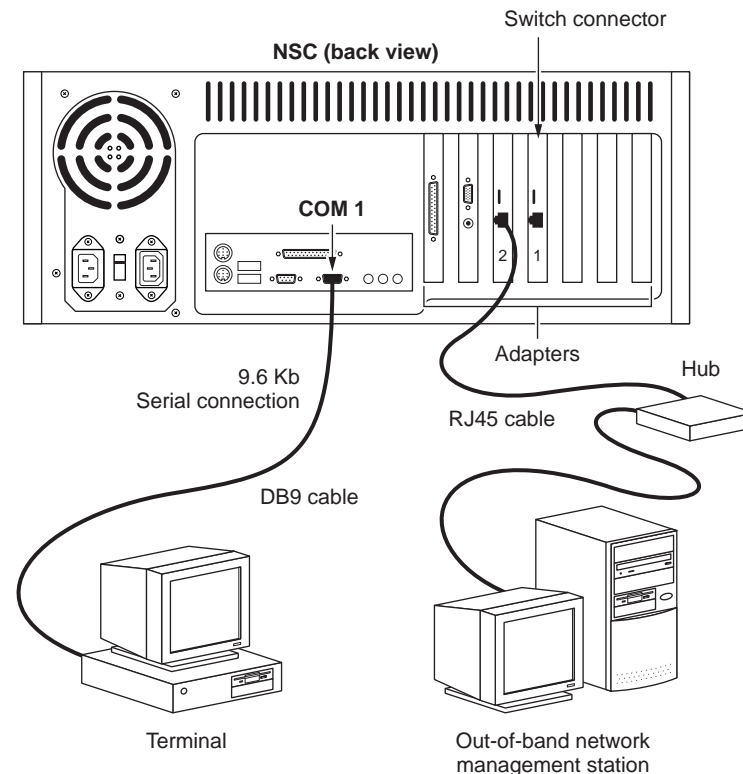
Note: You will be unable to log in on Com 2..

2. Make sure the terminal's setup parameters match those shown in the illustration.

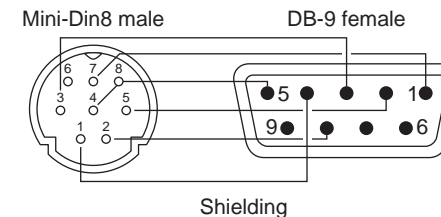
Caution: Follow the instructions in the diagram to establish the correct setup parameters on the terminal connected to the COM1 on the NSC. **Make sure you set the speed to 9.6Kb.** You may be unable to establish a connection to the switch during Startup, unless parameters are set correctly.

3. Connect a network management station to the NSC's Adapter 2 when you require an out-of-band Ethernet connection to the NSC.

Note: Use the correct cable when connecting equipment. Use a crossover cable to directly connect *similar* equipment: network-to-network (a hub to a switch) or client-to-client. It cross-connects pins (pin 1 to pin 3, and pin 2 to pin 6). Use a straight cable to directly connect *dissimilar* equipment: client-to-network (a management station to a hub or switch). It straight-connects pins (pin 1 to pin 1, pin 2 to pin 2, pin 3 to pin 3, and pin 6 to pin 6).



Setup Parameters	
Speed	9.6Kb
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None



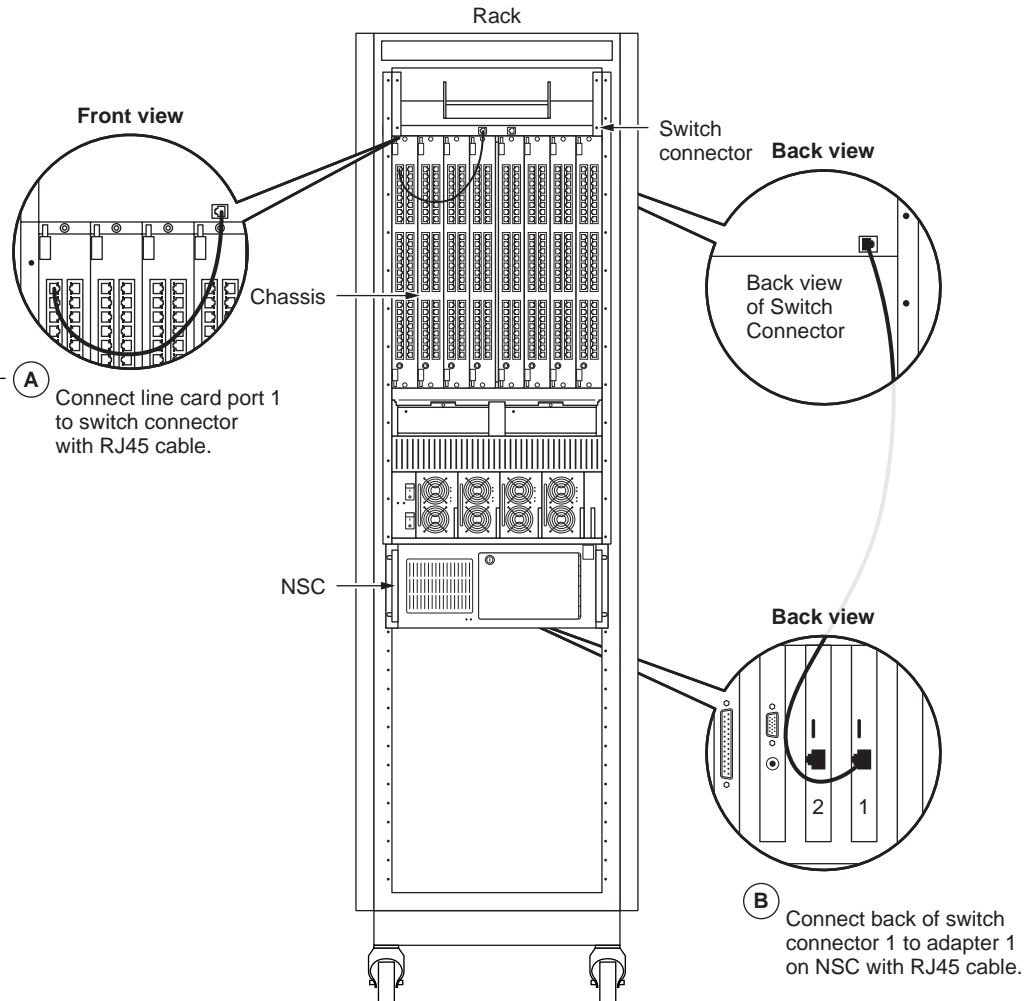
Connecting a Terminal and Management Station to the NSC

2.9 Connect the NSC to the Switch Chassis

After connecting the terminal and management station to the NSC, connect the NSC to the switch.

1. Connect line card port 1 to one of the switch connectors on the top of the switch chassis using the short RJ-45 cable provided with the system.
2. Connect the back of the switch connector to Adapter 1 on the NSC using the long, RJ-45 cable provided with the system.

Note: The RJ-45 cable is a straight cable. It *straight*-connects pins (pin 1 to pin 1, pin 2 to pin 2, pin 3 to pin 3, and pin 6 to pin 6).



Connecting the NSC to the Switch Chassis

2.10 Power On the Switch Chassis

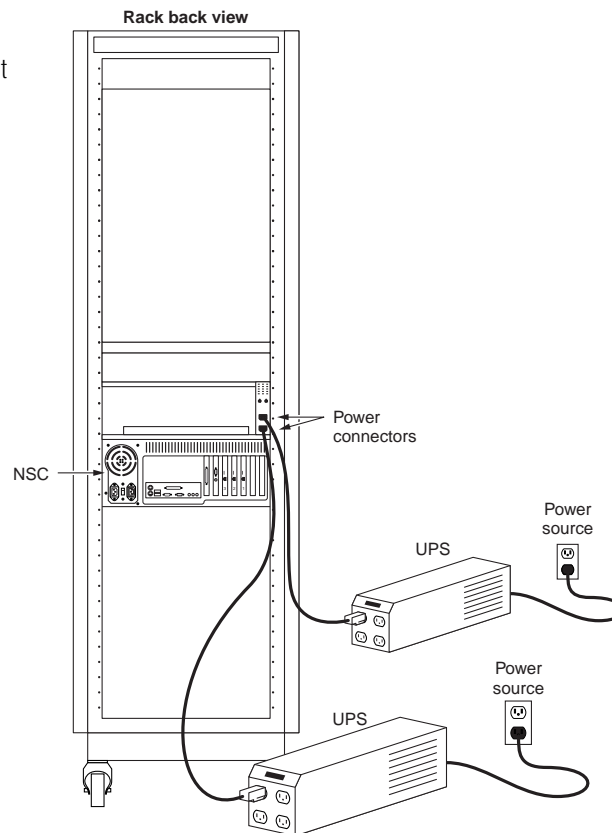
1. Using the power cord supplied with the system, connect the switch chassis to a power source.

We recommend that you:

- Connect the switch chassis to 2 separate circuits.
- Use Uninterruptible Power Supply (UPS) devices on both connections. The UPS will keep the system running if brownouts or short blackouts occur.

Warning

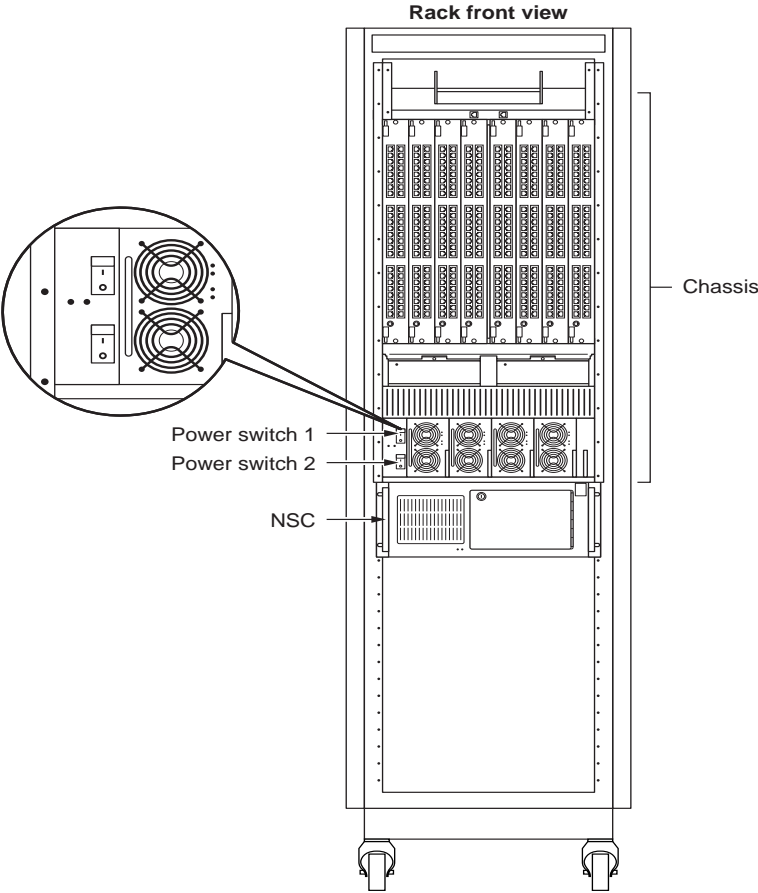
Do not put your hand inside the power supply enclosure while the machine is powered on because serious injury or death could result.



Powering On the Switch Chassis

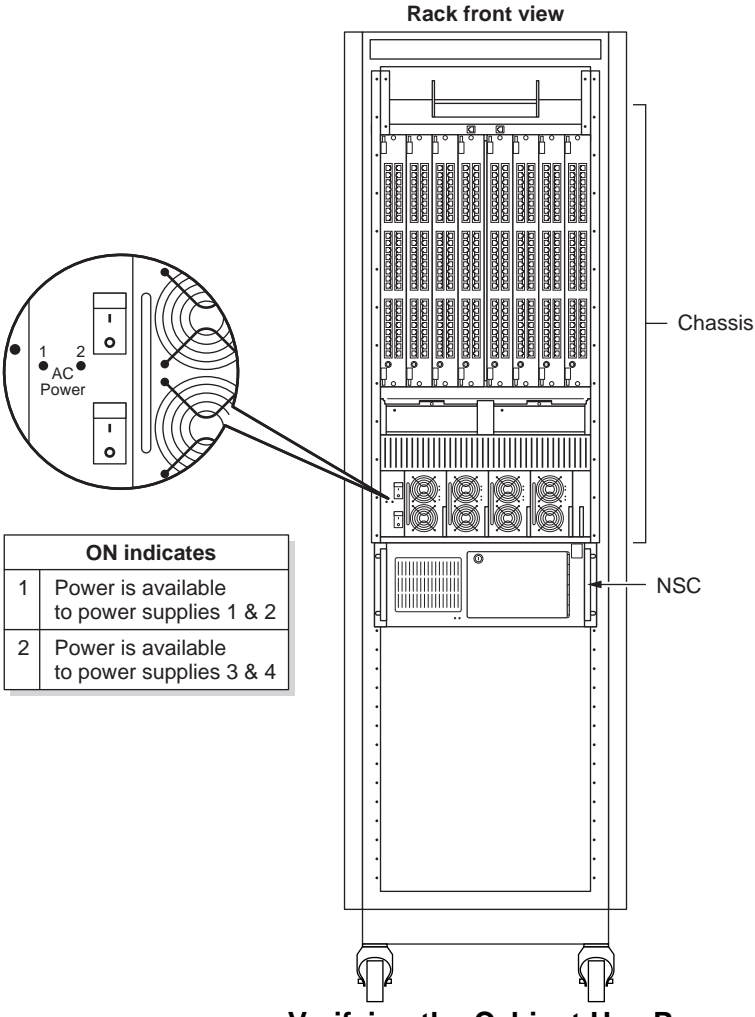
2.10 Power On the Switch Chassis
(continued)

2. Switch on power to the cabinet by moving both power switches to the On position.



Switching On Power to the Cabinet

3. Verify that the cabinet has power.

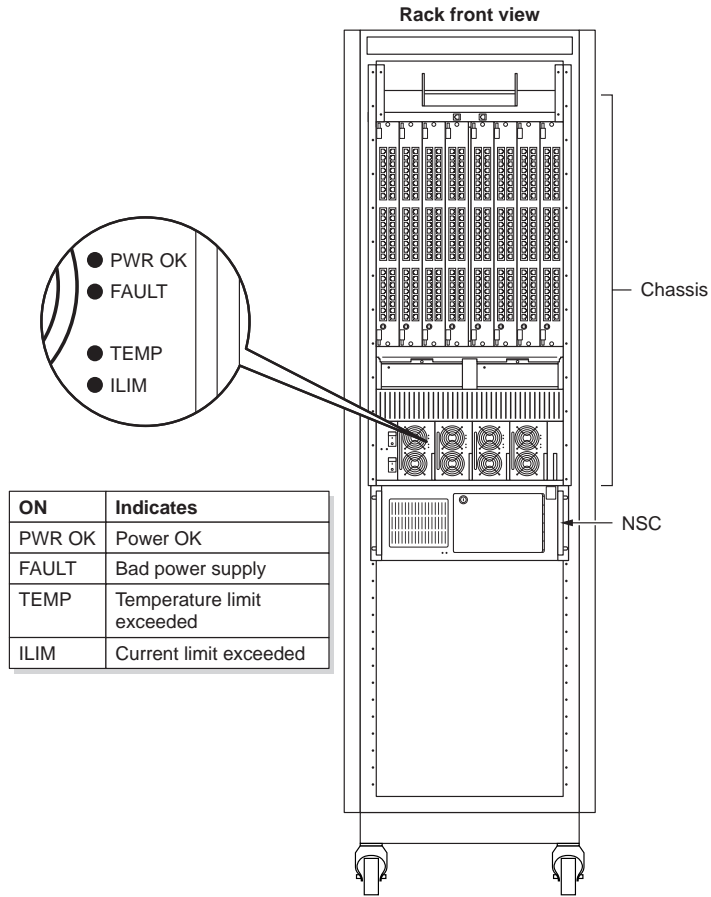


ON indicates	
1	Power is available to power supplies 1 & 2
2	Power is available to power supplies 3 & 4

Verifying the Cabinet Has Power

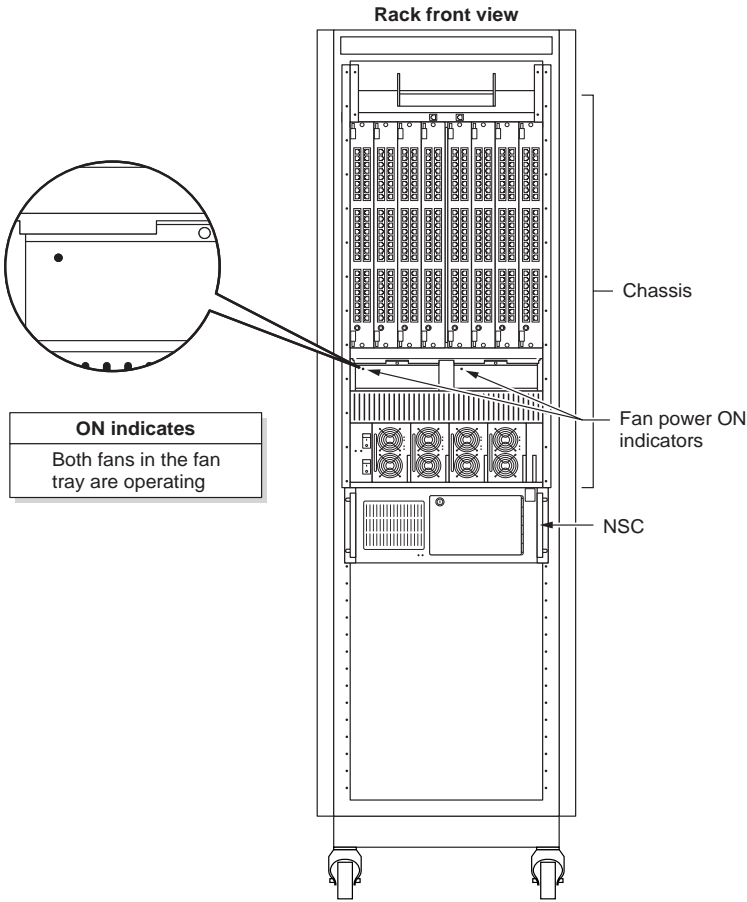
2.10 Power On the Switch Chassis
(continued)

4. Verify that each power supply is OK.



Verifying Power Supplies Have Power

5. Verify that the fans are OK.



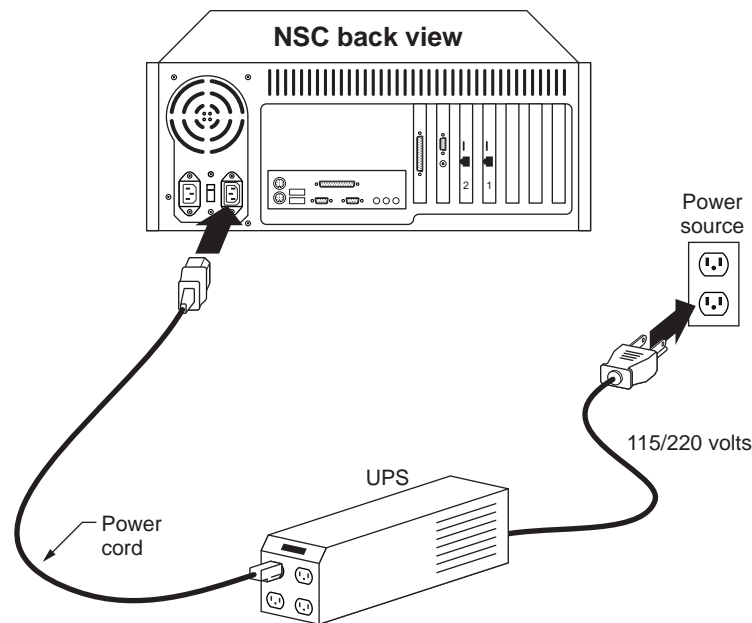
Verifying Fans Have Power

2.11 Power On the NSC, Terminal, and Management Station

1. Using the power cord supplied with the system, connect the NSC to a power source.

We recommend that you:

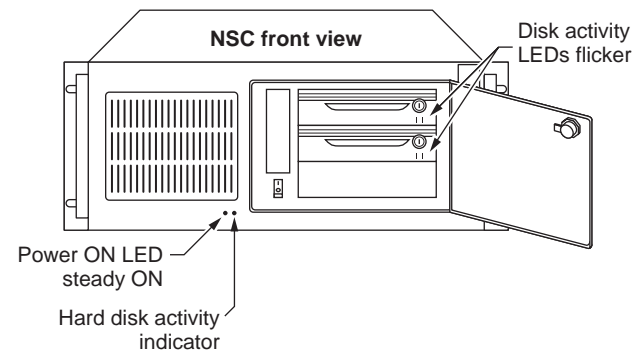
Connect the NSC to an uninterruptible Power Supply (UPS). The UPS will keep the NSC running if brownouts or short blackouts occur.



Connecting the NSC to Power

2. Power on the terminal and management station.

3. Verify that the terminal and the management station have power.
4. Switch on power to the NSC.
5. Verify that the NSC has power and that the disks on the NSC have power.

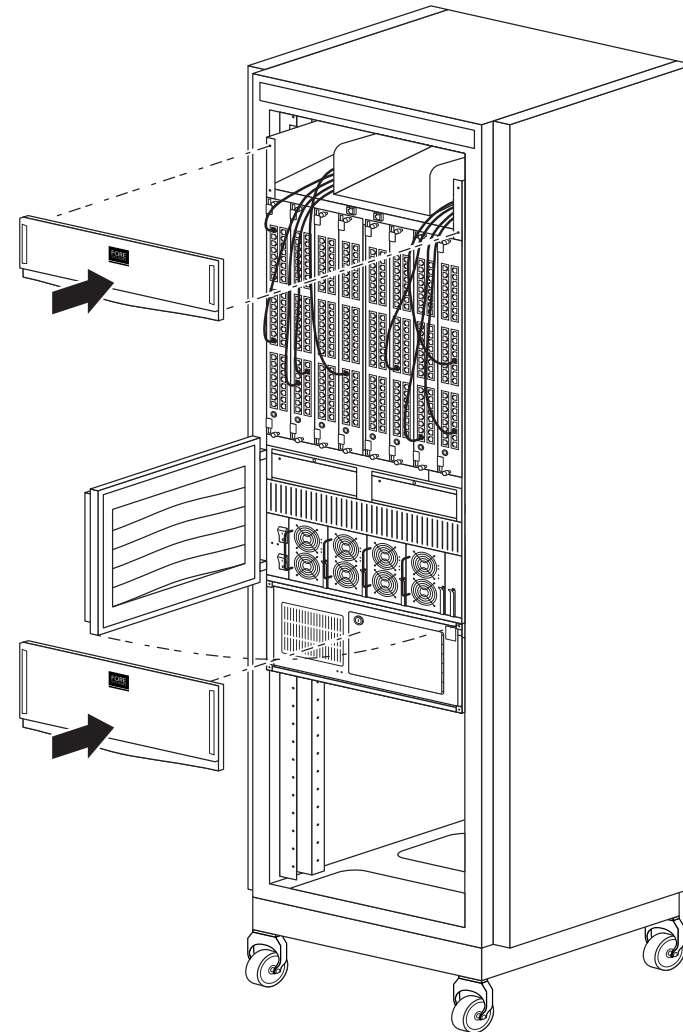


Powering on the NSC and Verifying the NSC and Disks Have Power

2.12 Install the Switch Covers

When installation is complete, replace the covers and close the door on the chassis as shown in the illustration.

Go to Chapter 4, "Startup."



Install the Switch Covers

Before installing your system, make sure you've made the necessary preparations and have the necessary equipment. (See the Site Planning Checklist.)

Chapter 3 describes how to install the ESX-2400 Switch. It consists of the following sections. Together, they contain step-by-step procedures describing how to:

- 3.1 Unpack the Switch Modules
- 3.2 Inspect the Shipment
- 3.3 Unpack and Install the Integrated Stack
- 3.4 Install Switch Modules in the Integrated Stack
- 3.5 Install a Switch Module Directly in the Rack
- 3.6 Unpack and Install the NSC
- 3.7 Connect a Terminal and Management Station to the NSC
- 3.8 Connect the NSC to a Switch Module
- 3.9 Power On the Integrated Stack
- 3.10 Power On a Switch Module Installed in the Rack
- 3.11 Power On the NSC, Terminal, and Management Station

Introduction

Receiving Your Shipment

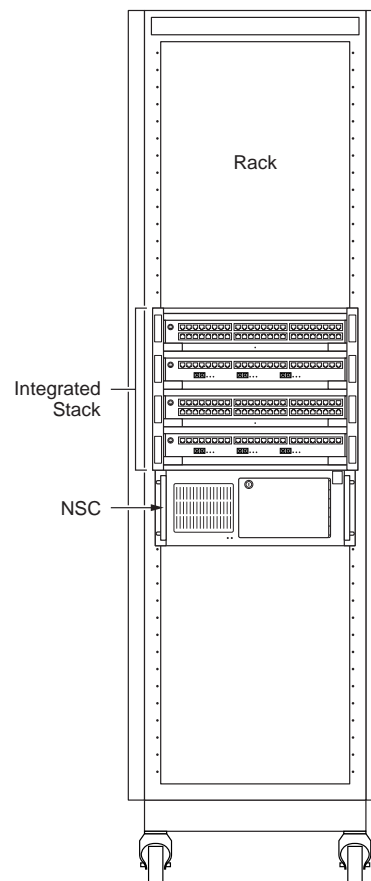
Before unpacking and signing off on the shipment, check the condition of the shipping container and make a note of any damage.

Using a pallet jack, move the shipping cartons containing your shipment close to the rack where you will install your ESX-2400 Switch.

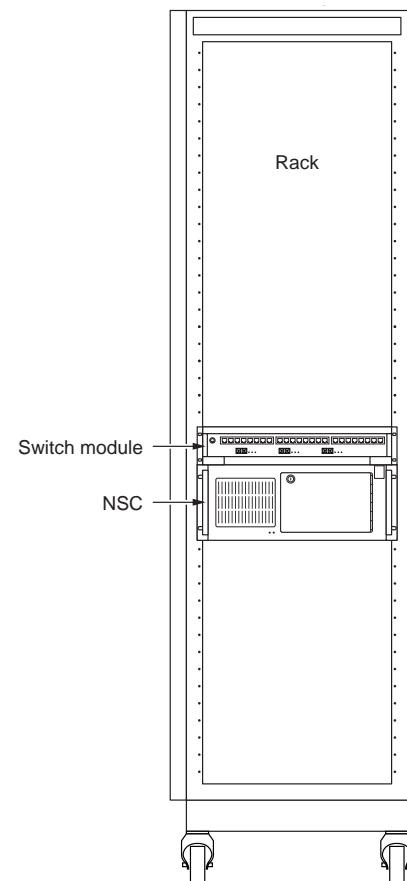
ESX-2400 Switch Configurations

Two ESX-2400 switch configurations are available: an Integrated Stack configuration that will hold up to four modules, and a single switch module configuration mounted directly in the rack. Both configurations come with a NSC that is mounted directly in the rack.

This chapter provides instructions for installing both configurations.



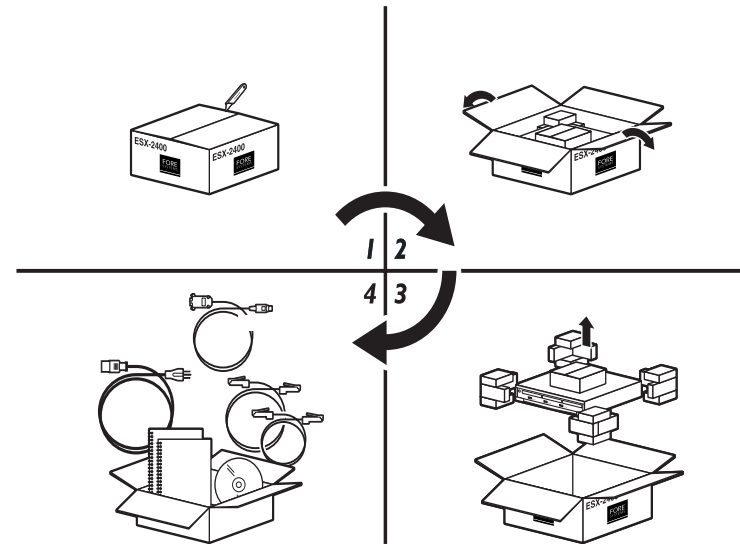
ESX-2400 Integrated Stack Configuration



ESX-2400 Single Switch Module Configuration

3.1 Unpack the Switch Modules

1. Carefully cut any tape securing the top flaps of the shipping carton containing the switch modules.
2. Fold back the flaps on the top of the box.
3. Remove any packing materials from the top of the box, and remove the accessory box containing the items described on the following page.
4. Leave the switch modules in the shipping carton until you install the Integrated Stack in the rack.

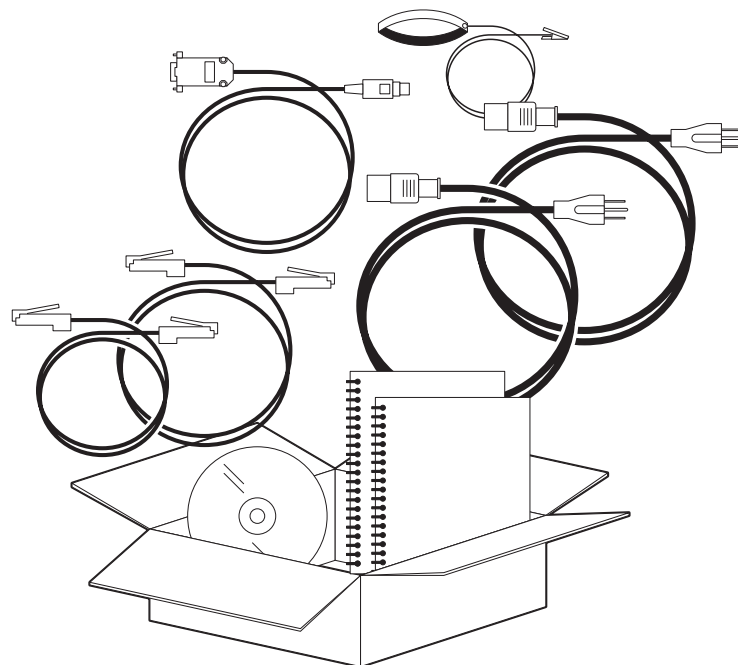


Unpacking an ESX-2400 Switch Module

3.2 Inspect the Shipment

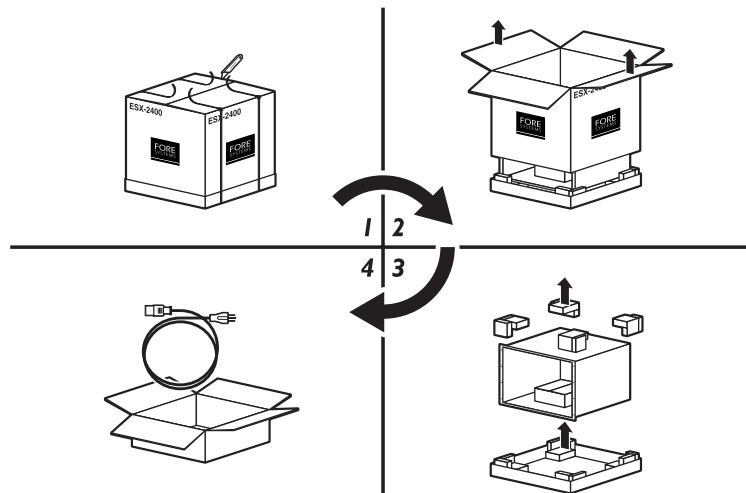
After unpacking the ESX-2400 switch modules, check the shipment:

1. Remove the cardboard box located inside the switch module shipping carton.
2. Open the box carefully and check the contents. The box should contain:
 - Switch module mounting brackets and screws
For mounting a switch module in the rack (optional)
Note: Mounting brackets and screws are not shown in the illustration.
 - Power cord
For powering a switch module and the NSC
 - RJ-45 cable
For connecting a switch module to the NSC
 - DB-9 serial cable
For connecting a terminal to the NSC's serial port
 - CD-ROM
For installing the ESX-Vision management software on a management station connected to the NSC
 - **Administrator Guide**
For learning to install, startup, and configure the switch using the ESX-Admin GUI management tool
 - **ESX-Cli Command Console Guide**
For learning to use the ESX-Cli command line management tool
3. Make a note of any damage or discrepancy and notify FORE Systems.



3.3 Unpack and Install the Integrated Stack

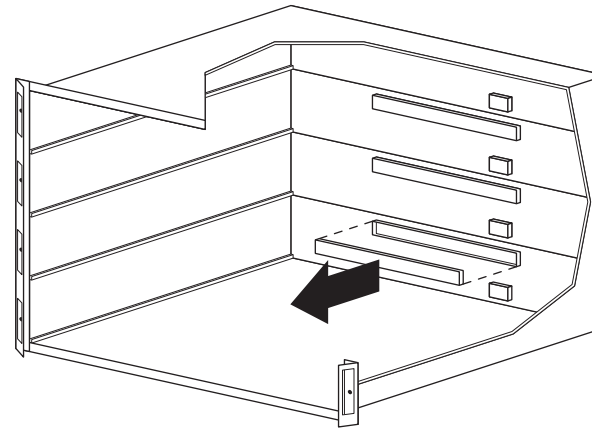
1. Locate the rack in a safe, clean, and accessible location. Make sure that the rack is level and that the wheels are locked before proceeding.
2. Remove the packing materials from the top of the box,
3. Lift and remove the Integrated Stack from the box.
4. Remove the two leverage brackets and the accessory box containing a power cord from inside the Integrated Stack.



Unpacking the ESX-2400 Stack

5. Remove the cover protecting the backplane from each slot where you plan to install a switch module.

To perform this step, twist the thumbscrews located on the ends of the protective cover in a counter-clockwise direction. Then remove the protective cover from the Integrated Stack.



3.3 Unpack and Install the Integrated Stack (continued)

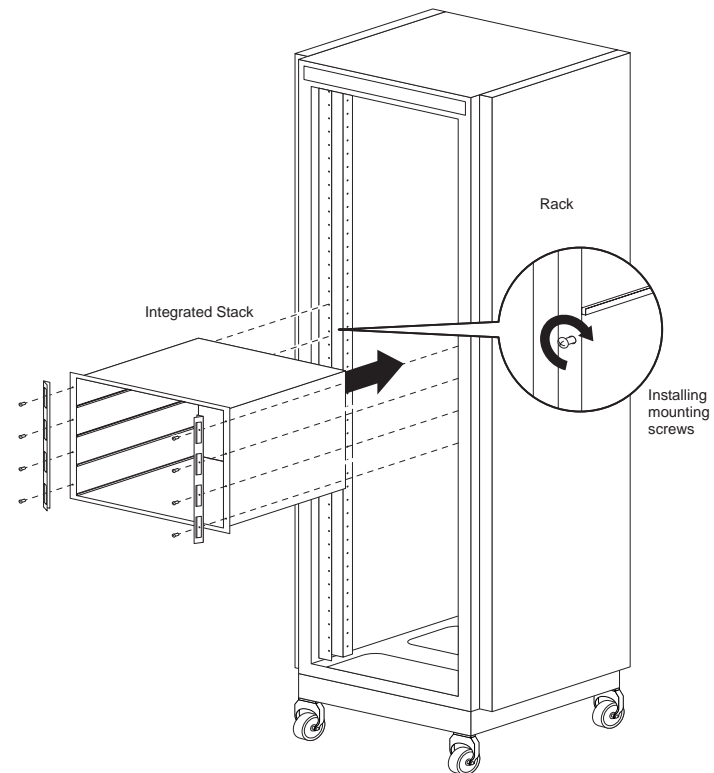
1. After the protective covers are removed from the slots where you plan to install switch modules, lift the Integrated Stack and slide it into the rack.

Note: Make sure that you allow room in the rack to mount the NSC just below the Integrated Stack.

2. Position the two leverage brackets on either side of the Integrated Stack, with the finger cutouts angled inward as shown in the illustration.
3. Align the mounting holes in the leverage bracket and the Integrated Stack with the rack and fasten them to the rack with machine screws.

Locate the bar-coded numbered label on the front of the Integrated Stack. When you configure the switch, you will enter that number in the software.

Note: The ESX-2400 Integrated Stack is intended only for use with Berkeley Networks ESX-2400 switch modules.



3.4 Install Switch Modules in the Integrated Stack

1. Prior to installing a switch module in a slot in the Integrated Stack, make sure that the cover protecting the backplane on the Integrated Stack has been removed.

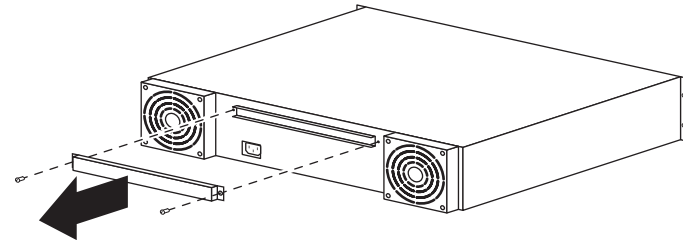
Caution: If you add a switch module later, unplug the Integrated Stack's power cord before reaching inside the Integrated Stack to remove the cover protecting the backplane on the Integrated Stack.

Warning

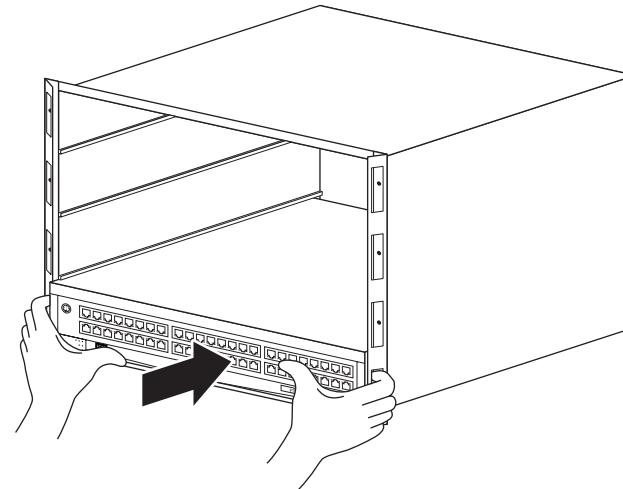
Do not put your hand inside the Integrated Stack enclosure while the machine is powered on because serious injury or death could result.

2. Remove a Switch module from its shipping carton.
3. Remove the screws holding the cover plate protecting the back plane connector on the switch module, and remove the cover plate.
4. Slide the switch module into the Integrated Stack, carefully.
5. Locking your fingers in the holes provided in the leverage brackets, press the switch module in snugly, using your thumbs to apply gentle, even pressure.

Repeat these steps until you have installed all the switch modules.



Removing the Cover Plate



Installing the Switch Module

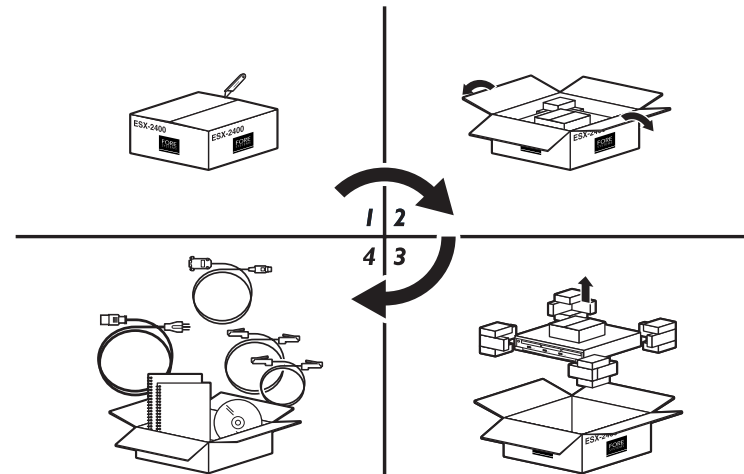
3.5 Mount a Switch Module Directly in the Rack

Note: This procedure describes how to mount a switch module directly in the rack. This procedure applies only to the single-switch-module configuration.

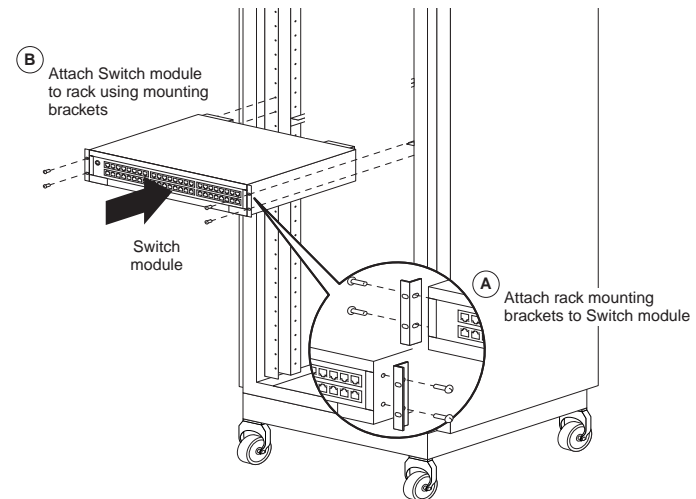
1. Remove the switch module from the shipping carton.
2. Attach two rack mounting brackets to the switch module, one on each side near the front, using the machine screws provided.
3. Align the mounting holes in the brackets with the mounting holes in the rack and secure the switch module in the rack with machine screws.

Make sure that you allow room in the rack to mount the NSC just below the switch module.

Note: Locate the bar-coded numbered label on the back of the switch module. When you configure the switch, you will enter that number in the software. This number can be read from the console.



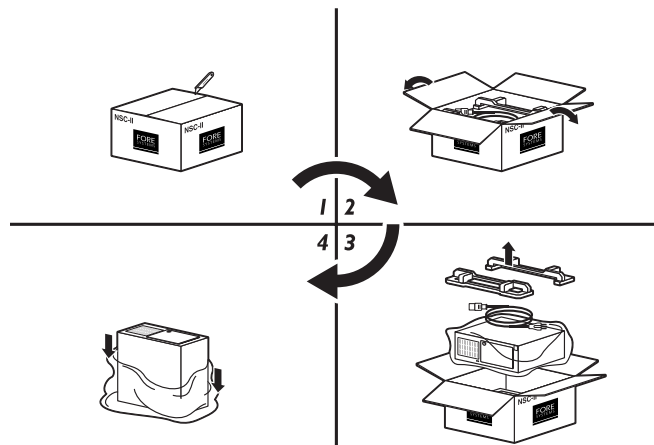
Unpacking an ESX-2400 Switch Module



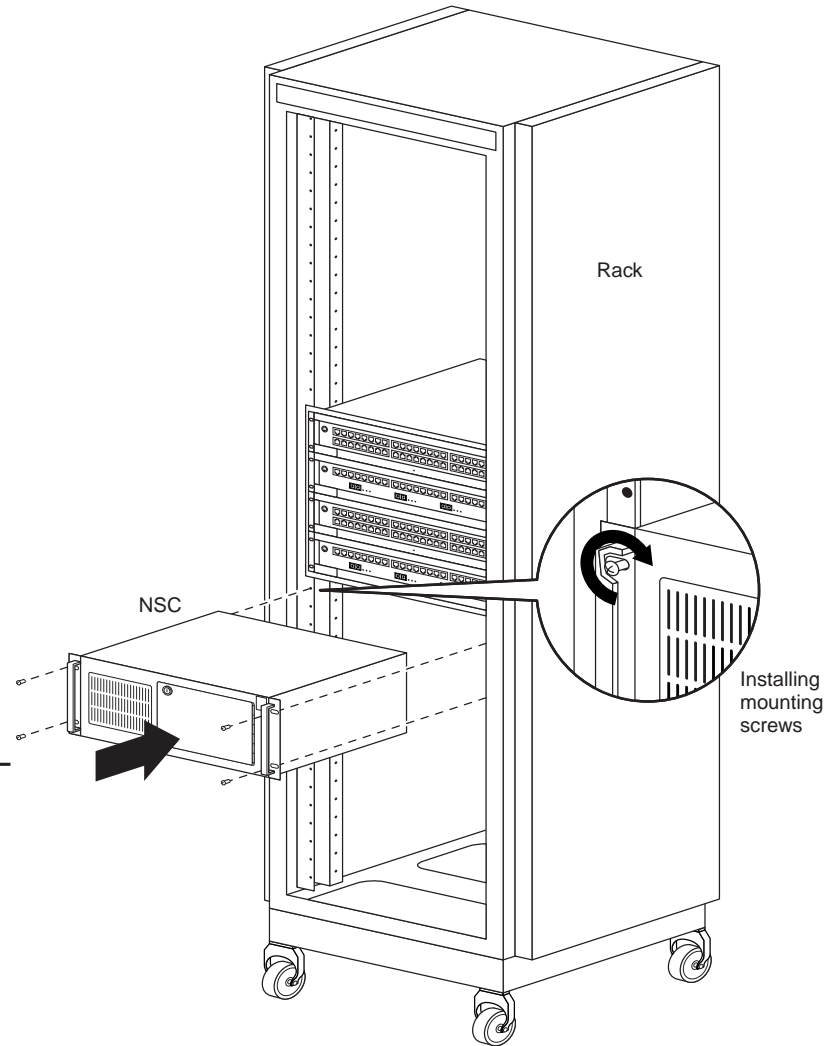
Installing an ESX-2400 Switch Module

3.6 Unpack and Install the NSC

1. Carefully cut any tape holding the top flaps of the shipping carton together.
2. Fold back the flaps on the top of the box.
3. Remove the packing materials and the power cord from the top of the box.
4. Remove the NSC from the shipping carton.
5. Remove the plastic bag protecting the NSC.
6. Lift the NSC, and position the NSC in the rack.
7. Align the mounting holes and secure the NSC in the rack with machine screws.



Unpacking the NSC



Installing the NSC

3.7 Connect a Terminal and Management Station to the NSC

After mounting the chassis and the NSC in the rack, follow these instructions to connect a terminal and management station to the NSC. You can use a single device as both a management station and a terminal:

1. Connect a terminal to the NSC's Com 1 serial port using a DB9 null modem cable—required to startup the system. See Section 4, "Startup".

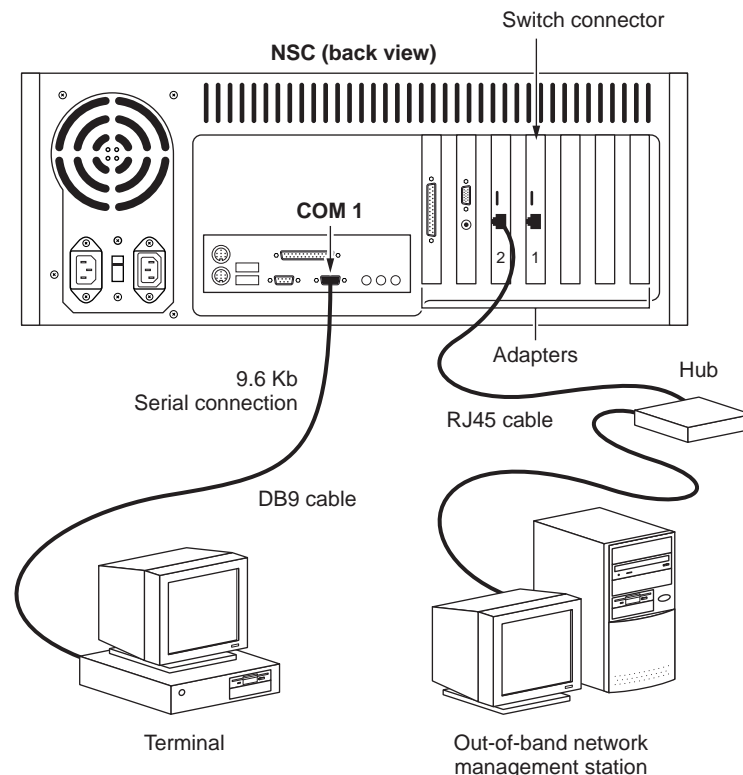
Note: You will be unable to log in on Com 2..

2. Make sure the terminal's setup parameters match those shown in the illustration.

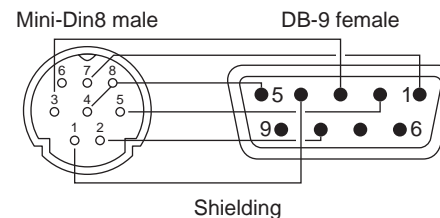
Caution: Follow the instructions in the diagram to establish the correct setup parameters on the terminal connected to the COM1 on the NSC. **Make sure you set the speed to 9.6Kb.** You may be unable to establish a connection to the switch during Startup, unless parameters are set correctly.

3. Connect a network management station to the NSC's Adapter 2 when you require an out-of-band Ethernet connection to the NSC.

Note: Use the correct cable when connecting equipment. Use a crossover cable to directly connect *similar* equipment: network-to-network (a hub to a switch) or client-to-client. It cross-connects pins (pin 1 to pin 3, and pin 2 to pin 6). Use a straight cable to directly connect *dissimilar* equipment: client-to-network (a management station to a hub or switch). It straight-connects pins (pin 1 to pin 1, pin 2 to pin 2, pin 3 to pin 3, and pin 6 to pin 6).



Setup Parameters	
Speed	9.6Kb
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None



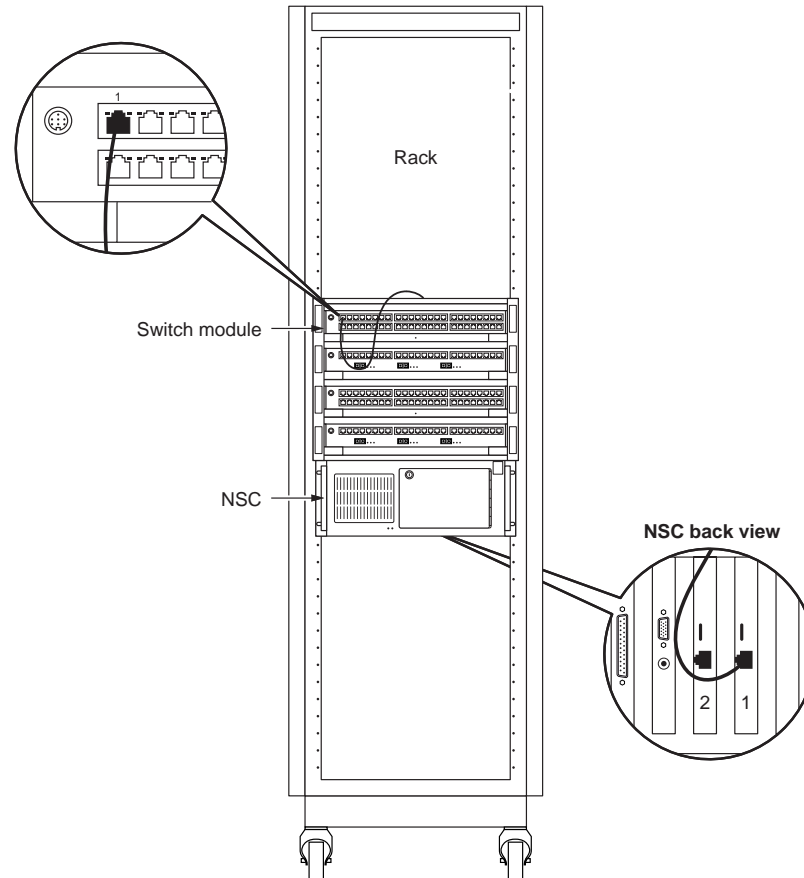
Connecting a Terminal and Management Station to the NSC

3.8 Connect the NSC to a Switch Module

After connecting the terminal and management station to the NSC, connect the NSC to a switch module.

Connect Port 1 (the connector on the top left of the switch module) to Adapter 1 on the NSC using the RJ-45 cable provided with the system.

Note: The RJ-45 cable is a **straight** cable. It *straight*-connects pins (pin 1 to pin 1, pin 2 to pin 2, pin 3 to pin 3, and pin 6 to pin 6).



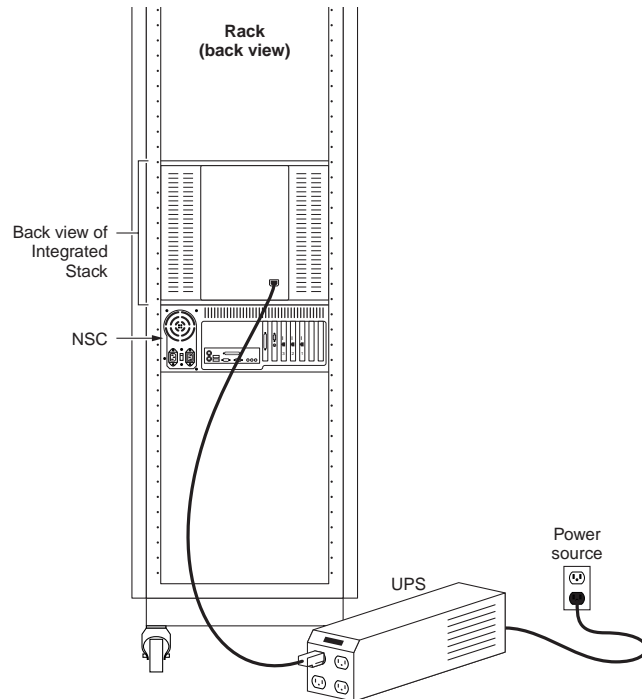
Connecting the NSC to a Switch Module

3.9 Power On the Integrated Stack

1. Connect the Integrated Stack to a power source using the power cable supplied with the Integrated Stack.

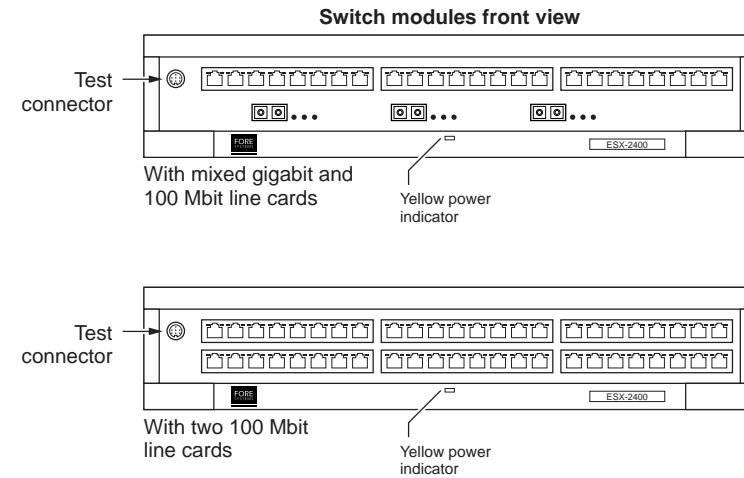
We recommend that you:

Connect the Integrated Stack to an Uninterruptible Power Supply (UPS). The UPS will keep the system running if brownouts or short blackouts occur.



Connecting the Integrated Stack to a Power Source

2. Verify that the Integrated Stack has power.
An LED behind the Berkeley Networks logo on the front of each switch module will turn ON.



Verifying the Integrated Stack Has Power

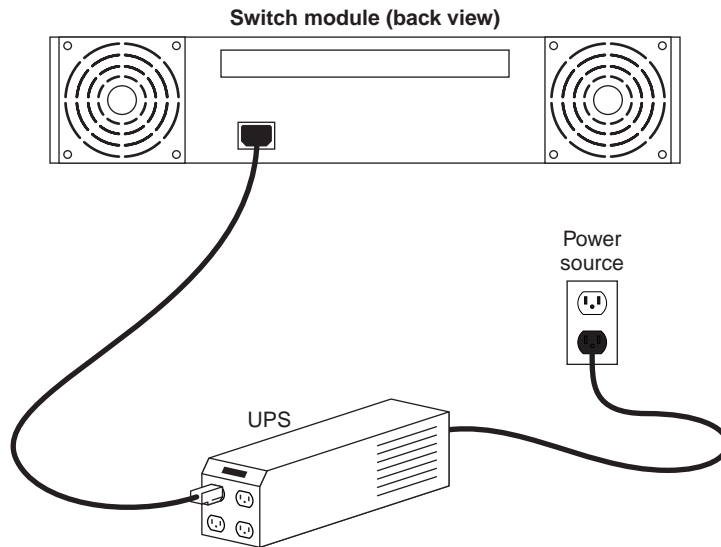
3.10 Power On the Switch Module Mounted in the Rack

This section describes how to power on a switch module mounted directly in the rack.

1. Connect the switch module mounted in the rack to a power source using a power cord supplied with the switch module.

We recommend that you:

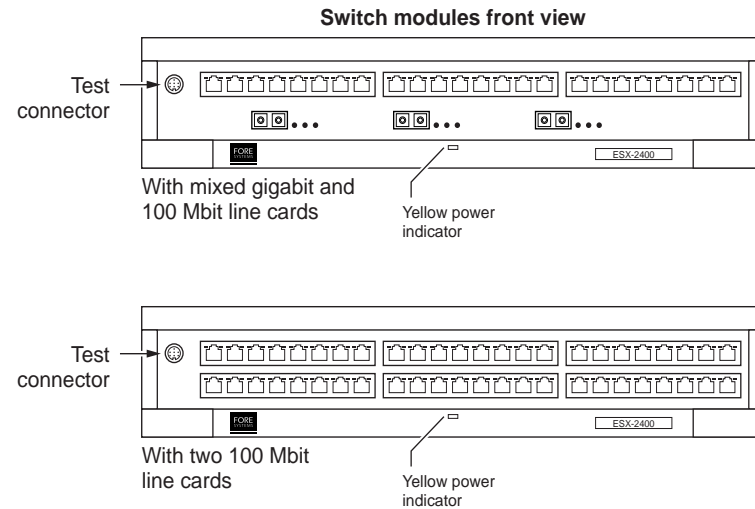
Connect the chassis to an Uninterruptible Power Supply (UPS). The UPS will keep the system running if brownouts or short blackouts occur.



Connecting the Switch Module to a Power Source

2. Verify that the switch module has power.

An LED behind the Berkeley Networks logo on the front of the switch module will turn ON.



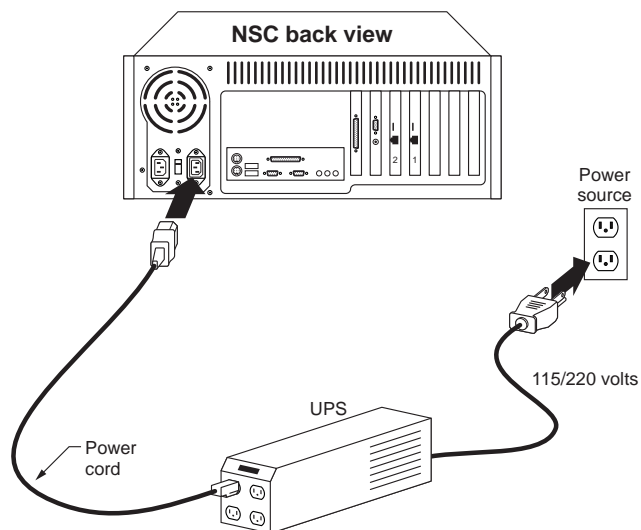
Verifying the Switch Module Has Power

3.11 Power on the NSC and Terminals

1. Connect the NSC to a power source.

We recommend that you:

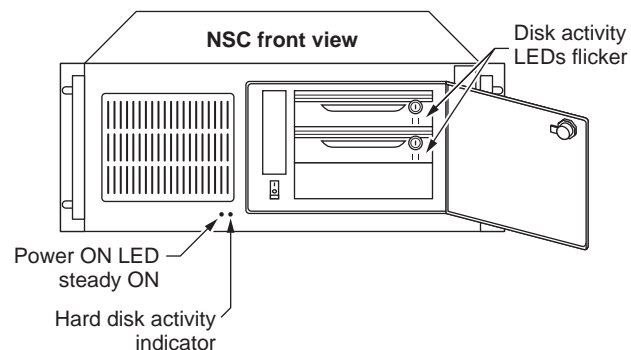
Connect the chassis to an Uninterruptible Power Supply (UPS). The UPS will keep the system running if brownouts or short blackouts occur.



Connecting the Switch Module to a Power Source

2. Power on the Terminal and the Network Management Station.
3. Verify that the terminal and management station have power.

4. Switch on power to the NSC.
5. Verify that the NSC has power and that the disks on the NSC have power.



Powering On and Verifying the NSC Has Power

Go to Chapter 4, "Startup."

Before following instructions in this section, make sure that you have installed and powered up your system successfully. Startup consists of the following sections:

- 4.1 System Overview
- 4.2 Startup Sequence
- 4.3 Connect User Equipment to the Switch
- 4.4 Start the Management Software

System Overview provides a brief description of the ESX Switch.

Startup Sequence, guides you in establishing a control path between the NSC and the switch and management paths you can use to manage the switch.

Connect User Equipment to the Switch describes how to: connect the NSC's control port and the switch, connect user equipment to switch ports, and verify that ports are operating normally.

Start the Management Software describes how to load software on a management station connected to Adapter 2 on the NSC. This will allow you to configure the switch using ESX-Admin, a GUI management interface.

Once startup is complete, you can configure the switch. See the following chapters for details.

4.1 System Overview

Startup occurs after Installation. It assumes that you have completed the following tasks:

- ☐ Bolted the system in a rack
- ☐ Connected the cables
- ☐ Powered up the system
- ☐ Connected the NSC to the switch
- ☐ Connected a terminal to the NSC's serial port

4.1.1 Switch Operating Characteristics

The switch provides frame forwarding at these connection speeds:

- 10 BaseT
- 100 BaseT
- 1000 BaseT

The switch provides three layers of switching:

- Layer 2–bridging
- Layer 3–routing
- Layer 4–application-aware switching

4.1.2 Switch Components

The switch consists of two main components. A Hardware Forwarding Engine (HFE) receives and forwards packets. A Network Service Controller (NSC) tracks network changes and keeps the HFE informed as network changes occur.

4.1.3 Control and Management Paths

The dual purposes of Startup are to enable the control and management interfaces. *See the following illustration for details.*

Control Path

The **control path** between the NSC's **adapter 1** and a port on the HFE transfers control information from the NSC to the HFE and returns status information to the NSC.

Management Paths

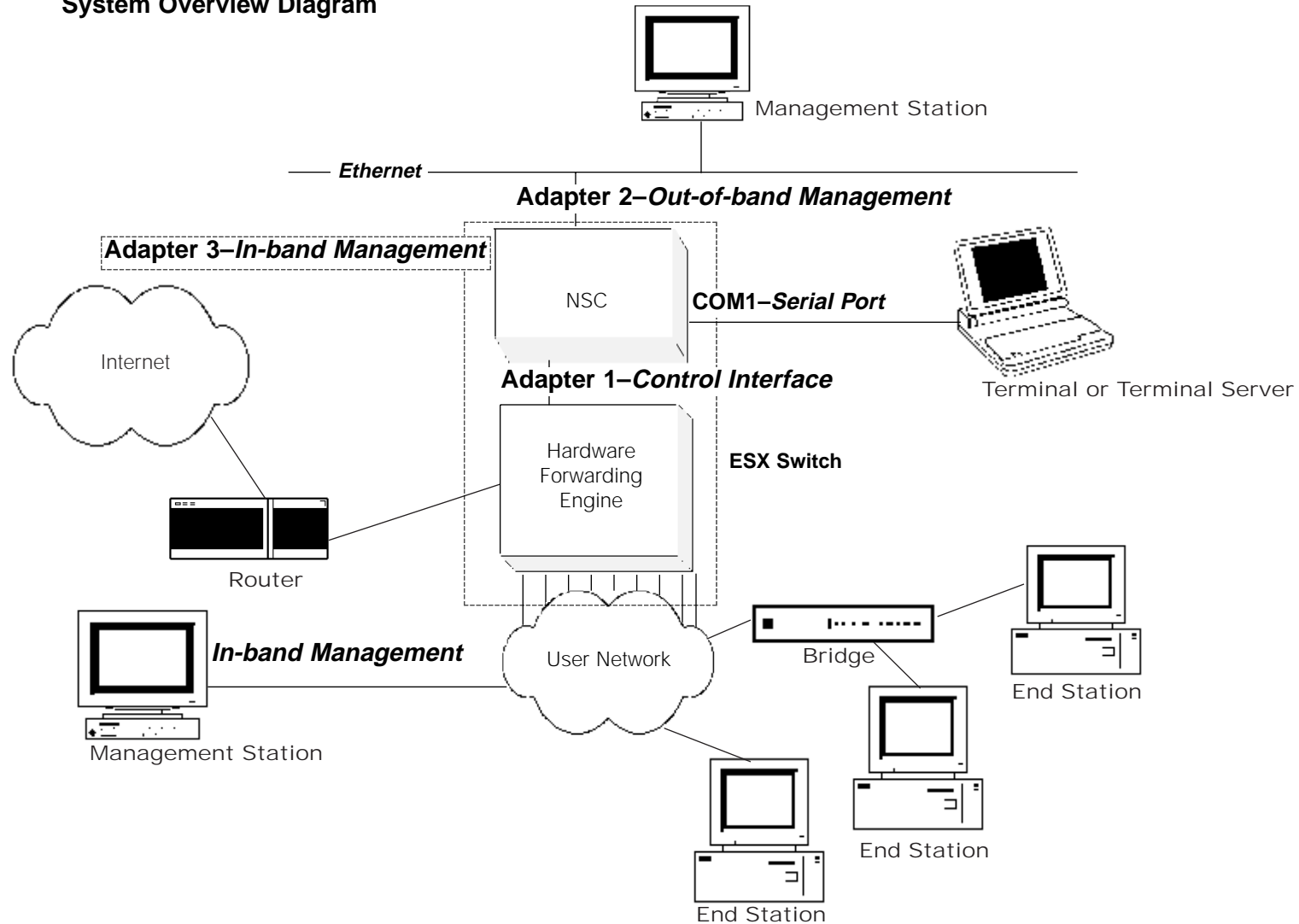
The management paths to the ESX Switch allow you to manage the switch via the following connections:

- **Serial port connection**—via the NSC's **COM1** port
During startup, used for enabling the control interface as well as out-of-band and in-band management interfaces. *Supports only the command line interface.*
- **Out-of-band connection**—via the NSC's **adapter 2**
Used for configuring and managing the switch and displaying switch status. *Supports command line & GUI interfaces.*
- **In-band connection**—via one of the ports on the switch.
Used for configuring and managing the switch and displaying switch status.
Note: As described in Section 4.2, the in-band connection is made possible by assigning an internal IP address for the NSC on **adapter 3**.
Supports command line & GUI interfaces.

4.1.4 Connecting User Equipment to the Switch

As shown in the following diagram, the ESX Switch provides connections between end stations, bridges, and routers that are attached to the user network or directly connected to the switch.

System Overview Diagram



4.2 Startup Sequence

The Startup Sequence begins when you attach a terminal to the NSC's COM1 port and issue ESX-Cli commands. It concludes when you have established the control and management paths you will need to operate and manage the switch.

During the Startup Sequence, using a terminal connected to the NSC's serial port, you will establish the following control and management paths:

- **control path** between the NSC and the switch chassis—via the NSC's **adapter 1**
- **out-of-band management path** via the NSC's **adapter 2**.
- **in-band management path** via the NSC's **adapter 3**.

Note: To manage the switch in-band, you must assign an IP address to one of the ports on the switch. See Section 4.4.2, "Startup Procedure", Step 9.

When the Startup Sequence is complete, you can connect user equipment to the switch and load the management software that will allow you to manage the switch from a management station. These tasks are described in the remaining sections of Chapter 4.

4.2.1 Startup Sequence Overview

This section provides an overview of the steps that are described in detail in the following section.

1. Establish terminal-to-NSC path

Allows the NSC to communicate with the switch.

2. Limit control ports

Restricts the number of ports on the switch that can be used as control ports.

3. Name the NSC

Assigns a node name to the NSC that allows it to be accessed.

4. Change default password

Provides a means of restricting access to the switch.

5. Configure out-of-band management interface

Establishes a path for managing the switch using a management station connected to the NSC's **adapter 2**.

6. Configure internal IP address

Establishes an IP address for the NSC's **adapter 3**.

This address is the internal IP address of the switch. It enables the switch to be managed in-band, via a management station connected to the user network.

Note: **Adapter 3** provides a *logical not* a *physical* connection to the NSC.

7. Reboot

Causes the new name for the NSC established in Step 3 to take effect.

8. Configure in-band management path

Establishes an in-band management path to the network that contains the NSC's internal IP address for **adapter 3**.

4.2.2 Startup Procedure

The Startup Procedure follows:

1. Establish terminal-to-NSC path

- Connect a terminal to NSC
(displays a logon prompt) logon:
- Enter default logon logon: **administrator**
- Enter default password <CR>..... password: <CR>
- Displays CLI> prompt..... CLI>

2. Limit NSC ports

- Limit NSC ports to 1A1 CLI> **cfg bsc mgt-only port 1a1**
Connected to remote node (nsc-master.\\.\com1)
- Add backup NSC port 1A2 CLI> **cfg bsc mgt-add port 1a2**
- Verify NSC port configuration CLI> **show bsc cfg**

config number of entries: (1) node: (nsc-test3)

 Slot NSC Ports
 1 1A1, 1A2

3. Name the NSC

- Give the NSC a unique name CLI> **name <unique name>**up to 15 alpha/numeric characters

Note: WINS is enabled on adapters 2 and 3. By naming the NSC, you allow the NSC to be reached by its node name in addition to its IP address.

4. Change default password

- Enter password command..... CLI> **cfg nsc account administrator**
- Enter new password Enter Password: ****
- Enter new password again Verify Password:

5. Configure out-of-band adapter

- Set adapter 2's IP address CLI> **cfg ip address 192.168.0.34 mask 255.255.255.0 adapter 2**

Note: The default address is: 192.168.0.1/24

- Verify adapter 2 configuration CLI> **show ip cfg adapter 2**

```
Adapter Configuration  Number of Entries: (1)  Node:(nsc-master.\\.\com1)

Address            Adapter  Mask                BCastAddr  Gateway  DHCP-Mode
192.168.0.34       2        255.255.255.0      0.0.0.0    0.0.0.0  Disabled
```

6. Configure internal IP address

- Set adapter 3's IP address CLI> **cfg IP address 192.168.1.1 mask 255.255.255.0 adapter 3**

- Verify adapter 3 configuration CLI> **show ip cfg adapter 3**

```
Adapter Configuration  Number of Entries: (2)  Node:(nsc-master.\\.\com1)

Address            Adapter  Mask                BCastAddr  Gateway  DHCP-Mode
192.168.0.34       2        255.255.255.0      0.0.0.0    0.0.0.0  Disabled
192.168.1.1        3        255.255.255.0      0.0.0.0    0.0.0.0  Disabled
```

7. Reboot

- Exit from ESX-Cli CLI> **exit**
- Restart ESX-Cli C:\winnt\system32>**esx-cli**

FORE Systems ESX-Cli Command Console
- Reboot the NSC CLI> **reboot**

8. Create in-band management path

You can manage the switch *locally* over a serial port using ESX-Cli, and you can manage it *remotely* using one of the following facilities:

- *Telnet*—You can Telnet to any switch port that has an IP address and enter ESX-Cli.
- *ESX-Cli and ESX-Admin*—To use these facilities, you must connect to a port that has windows networking enabled. On the NSC, two ports have windows networking enabled:
 - *Adapter 2*—the out-of-band adapter.
 - *Adapter 3*—the adapter containing the internal IP address of the switch.
To connect to adapter 3, a routed path must exist between your management station and the subnet configured on adapter 3.

Note: If you want to manage the switch over an OSPF or RIP network, refer to the following sections for instructions on configuring the adapter 3 interface:

- *Section 7.2, "Configuring OSPF".*
- *Section 7.3, "Configuring RIP".*

4.3 Connect Equipment to the Switch

In this section you will connect equipment to the HFE and verify that the user equipment is connected.

The following subsections provide step-by-step instructions to:

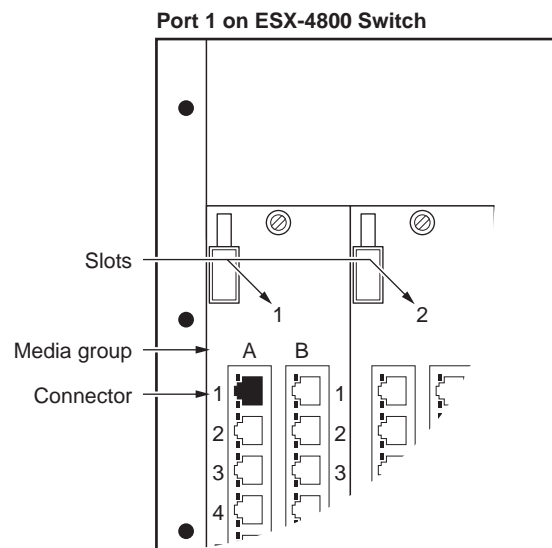
- Identify the Port Connected to the NSC
- Connect user equipment to HFE ports
- Check port LEDs

4.3.1 Identify the Port Connected to the NSC

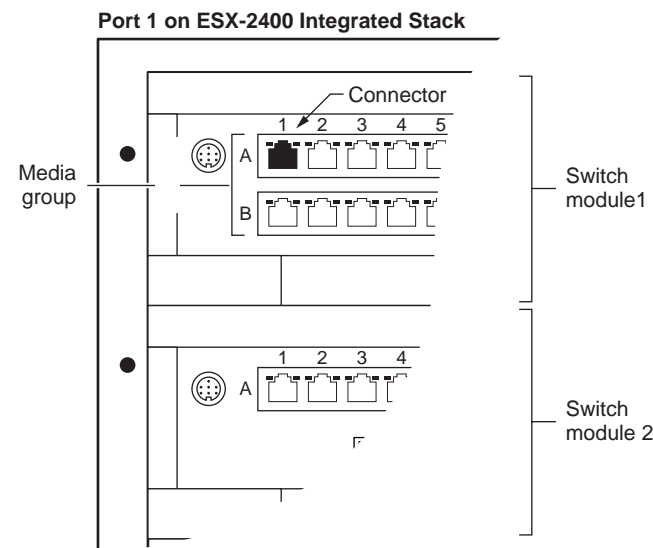
During installation, you connected a port on the Switch to the NSC. Write down the number of this Port.

We recommended that you connect Port 1 on the switch to the NSC, and use a different colored cable for this connection—making it easy to distinguish between the control port and user ports.

The following illustration shows where Port 1 is located on the ESX-4800 and ESX-2400 Switches:



Note: Port 1 on the ESX-4800 Switch is located on the upper left of the chassis.



Note: Port 1 on the ESX-2400 Switch is located on the upper left of the Integrated Stack.

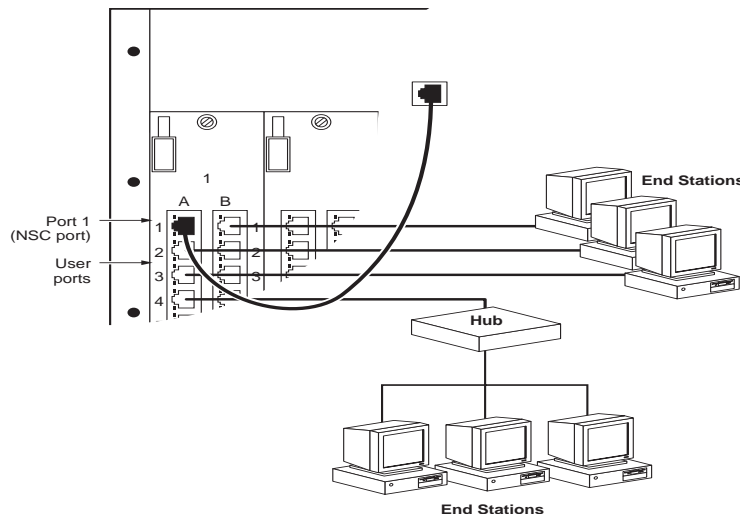
4.3.2 Connect User Equipment to Switch Ports

Using the appropriate Ethernet cables, connect user equipment to user ports on the HFE. Three types of Ethernet connections are supported:

- Cat-5 cables with RJ-45 connectors for 10/100 Base TX connections
- 50 μ or 62.5 μ multi-mode fiber cables with Duplex-SC connectors for 1000 Base SX short haul connections—up to 220 meters
- 9 μ single-mode fiber cables with Duplex-SC connectors for 1000 Base LX long haul connections—up to 5 kilometers

Note: You need to supply these cables. They are not provided with the system.

The following illustration shows user equipment connected to user ports on the ESX-4800 Switch. Generally, you will attach user equipment to the HFE via hubs.

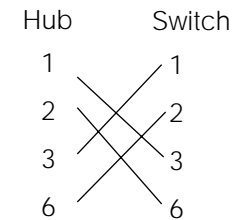


Special Requirements for Hub Connections

When you **connect a hub** to a switch you need to use a special cable, called a *crossover cable*.

A *crossover cable* cross-connects these pins:

- pins 1 to pins 3
- pins 2 to pins 6

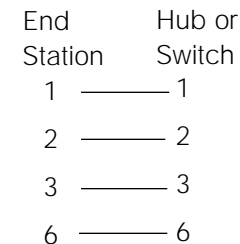


Crossover Cable

When you **connect an end station** to a hub or switch, use a standard, straight-through cable.

A *straight through cable* straight-connects these pins:

- pin 1 to pin 1
- pin 2 to pin 2
- pin 3 to pin 3
- pin 6 to pin 6



Straight-through Cable

Special Requirements for Fiber Connections

The fiber cable connectors on the switch are labeled following IEEE standards specifying color codes for fiber cables:

- **LX connectors** are labeled "SMF" in yellow to match the IEEE color specification for single-mode fiber cables.
- **SX connectors** are labeled "MMF" in orange to match the IEEE color specification for multi-mode fiber cables

Caution: When you connect fiber cables to the switch, make sure that you do not connect an LX cable to an SX connector, or vice versa.

- The connection will not perform properly.
- The mating tolerances on fiber connections are so tight that once connected, you may find that it is impossible to remove the cable.
- You may need to return the switch module for repair.

Caution: When the switch is powered on, do not look directly at the end of a fiber cable or at an open switch port. Laser light is being transmitted through the cables and ports.

4.3.3 Establish Compatible Speed and Mode Settings Special Requirements for Linked Ethernet Devices

By default, all ports on the switch autonegotiate to determine speed and mode.

Caution: Both link partners—local and remote devices—must be configured with compatible settings in order to establish a reliable link. If link partners are unable to communicate, verify that their settings are compatible.

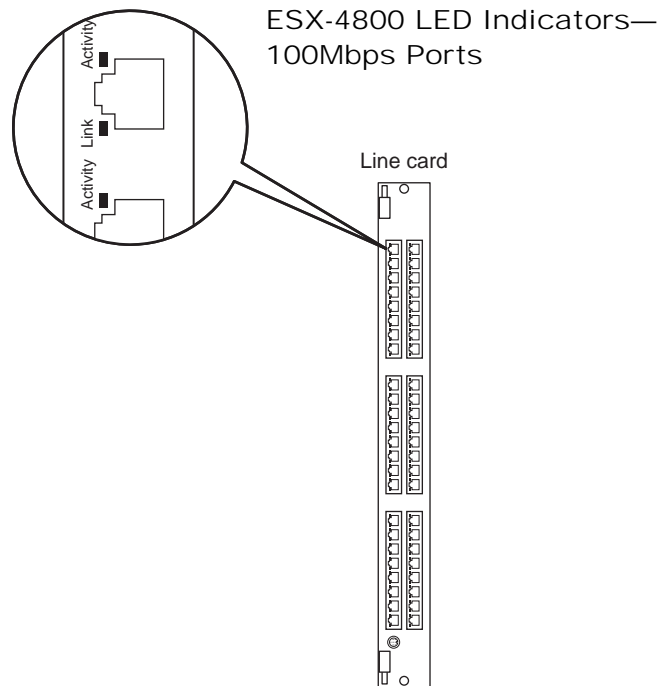
Note: 10/100 Base TX and Gigabit ports operate differently.

- 10/100 Base TX ports. can be configured to operate at either 10 or 100 Mbit speeds and in full or half duplex modes. *Refer to Section, 5.4.2, "Configure Ethernet Interfaces" for information on manually configuring 10/100 Base TX ports.*
- Gigabit ports can either autonegotiate or, if autonegotiation is disabled, they will operate at 1000 Mbit speed in full duplex mode—refer to the **ESX-Cli Command Console Guide** for information describing how to disable autonegotiation on gigabit ports.

4.3.4 Check Port LEDs

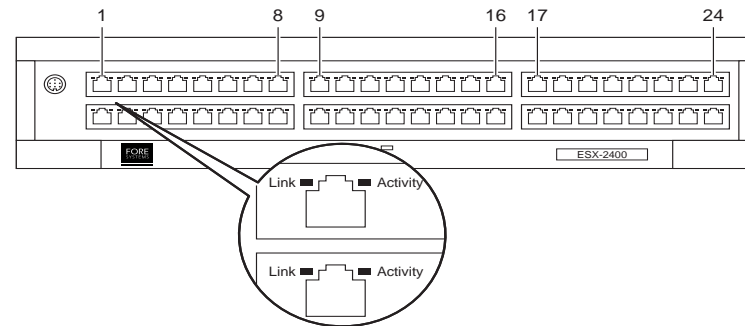
After connecting user equipment to user ports, check the port LEDs to verify that the ports are operating normally.

The following illustrations show the connectors available on the ESX-4800 and the ESX-2400 and their orientations. They also identify the LEDs and describe how to determine normal status.



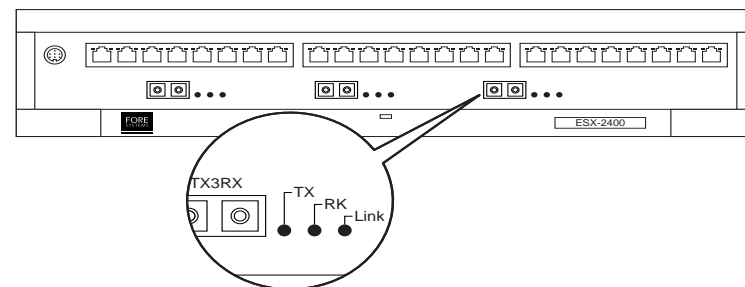
LED ON:	Indicates:
Link LED	Link established
Activity LED	Actively transmitting or receiving

ESX-2400 LED Indicators—100Mbps Ports



LED ON:	Indicates:
Link LED	Link established
Activity LED	Actively transmitting or receiving

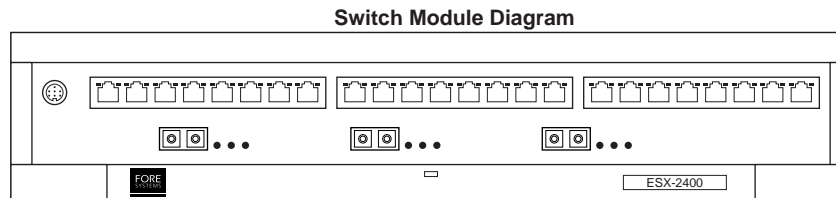
ESX-2400 LED Indicators—1000Mbps Ports



LED ON:	Indicates:
All 3 LEDs turn ON for 1/2 second then turn OFF	Successful power up
TX LED	Port is sending
RX LED	Port is receiving
Link LED	Link established

4.3.4 Check Port LEDs continued

During startup or normal operation the port LEDs may blink ON and OFF to indicate a problem condition. See the following diagram for details:



LED Failure Indications		
Blinking Port LED Pattern	Indicates	Corrective Action
Enabled LEDs blink ON and OFF	Switch is attempting to recognize an NSC	Make sure NSC cable is plugged into an enabled port
LEDs blink ON and OFF, moving right to left	At least one port failed the diagnostic loopback test	Swap the module
LEDs blink ON and OFF continuously, once, twice, or three times, then pause and repeat	Diagnostic test failure	Swap the module

4.4 Start the Management Software

After connecting user equipment to the switch, in this section you will install the management software on your network management station. After you install the management software and start it up, you can configure the system, described in the next chapters.

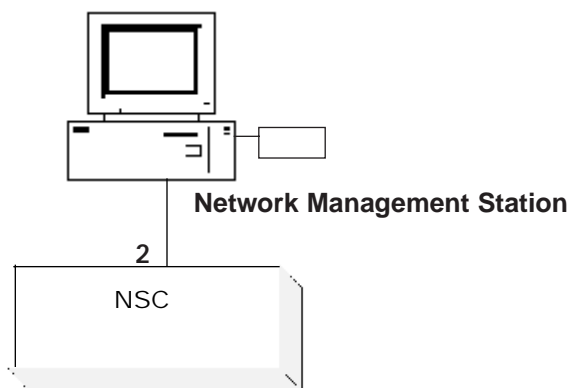
The following subsections provide step-by-step instructions to:

- Load management software
- Select the ESX-Admin management tool
- Access the chassis display

4.4.1 Load Management Software

Follow these instructions to load the CD containing the ESX-Vision software in your network management station connected to the NSC's Adapter 2.

Note: You must have Administrator privileges to load the management software, or the software will not create directories.

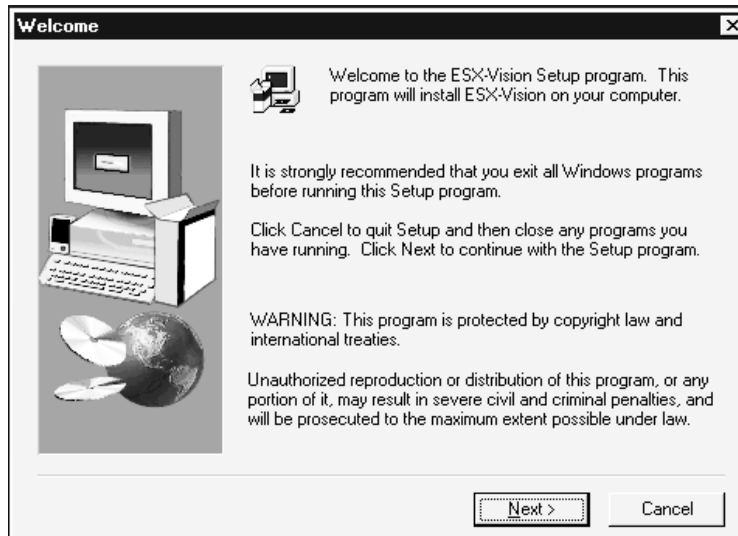


1. Load the ESX-Vision CD in the CD-ROM drive of your network management station.
2. Display the CD-ROM directory on your network management station.
3. Double-click the Setup.exe icon in the CD-ROM directory.
The system will start the ESX-Vision software installation wizard.

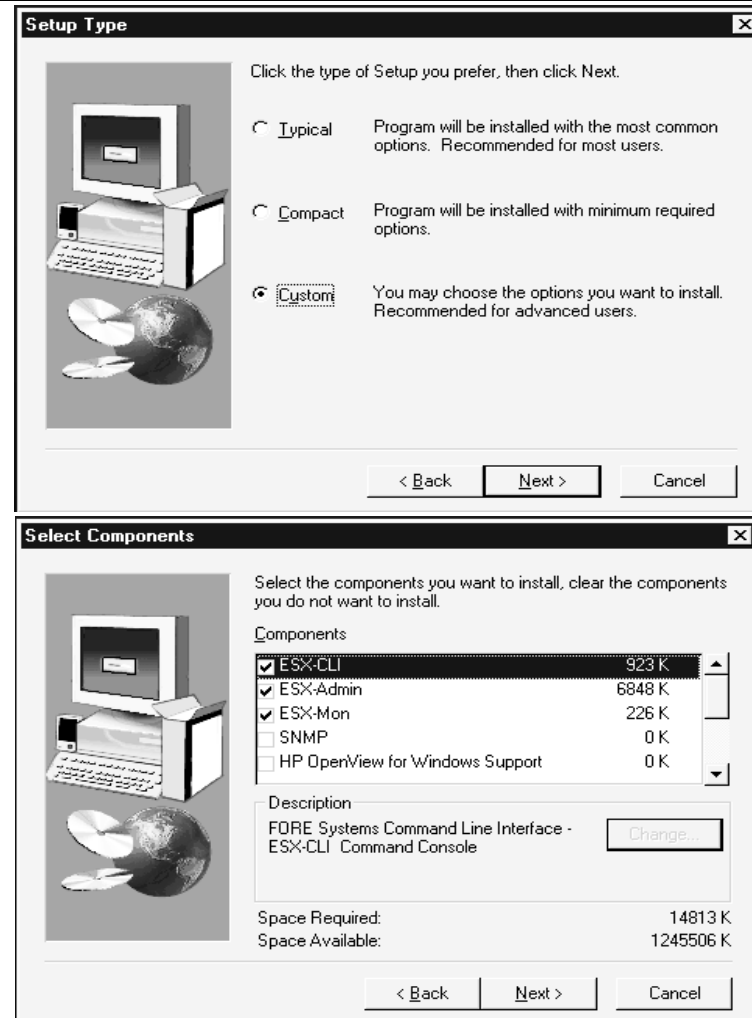
Name	Size	Type
inst32i.ex	284KB	EX_ File
_isdel.exe	8KB	Application
_setup.dll	11KB	Application Extension
_sys1.cab	228KB	CAB File
_user1.cab	230KB	CAB File
Data.tag	1KB	TAG File
data1.cab	9,692KB	CAB File
lang.dat	5KB	DAT File
layout.bin	1KB	BIN File
os.dat	1KB	DAT File
Readme_eVision.txt	8KB	Text Document
setup.bmp	97KB	Bitmap Image
Setup.exe	59KB	Application
Setup.ini	1KB	Configuration Settings
setup.ins	62KB	Internet Communicati...
setup.lid	1KB	LID File

4.4.2 Install the ESX-Vision Software on Your Network Management Station

Follow the instructions in the ESX-Vision installation wizard to install the ESX-Admin, ESX-Cli, and ESX-Mon management tools.



You can select a Typical, Compact, or Custom installation. Typical and Compact will install ESX-Cli, ESX-Admin and ESX-Mon. Custom will allow you to install software components by clicking the check box next to the component—see *the following screens for details*.

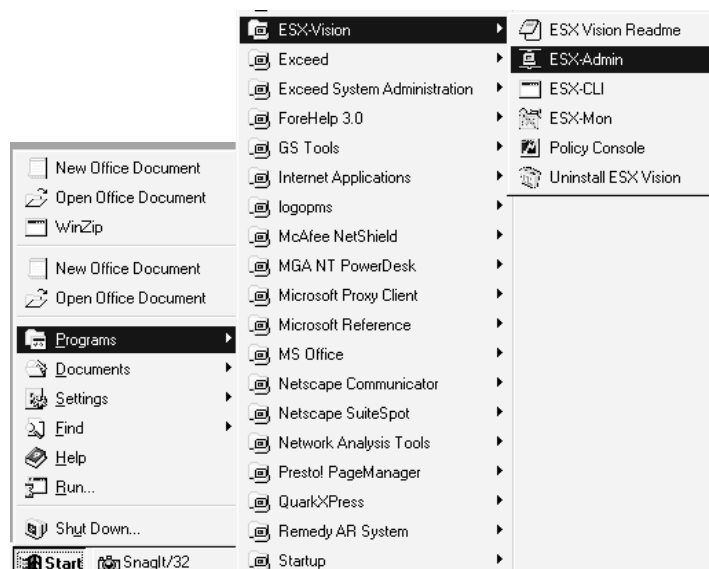


Note: When you move the scroll bar on the Components window, you can access additional components (including the Directory Console).

4.4.3 Start the ESX-Admin Management Tool

After installation, follow these steps to start the ESX-Admin management tool:

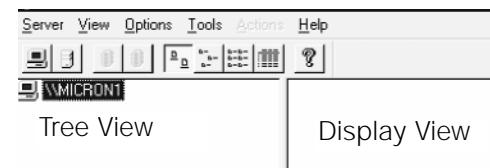
1. Open the Start Menu.
2. Select Programs.
3. Select ESX-Vision.
4. Select ESX-Admin.



ESX-Vision Management Program Menu

After you select the ESX-Admin icon, your network management station will display the Routing and RAS Admin screen, showing a tree view on the left and a display view on the right.

An icon representing your workstation will appear highlighted in the tree view.

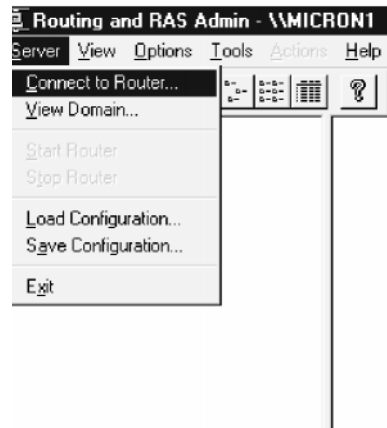


4.5 Access the Chassis Display

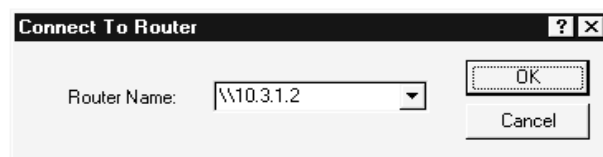
After starting the ESX-Admin software, you are ready to access the chassis display. This section provides step-by-step instructions.

After completing this section, you are ready to configure the system, described in Chapter 5.

1. Pull down the server menu and select "Connect to Router."
The system displays the Connect to Router pop-up window.



2. Enter the NSC name or IP address in the pop-up window (QUASAR in the example).



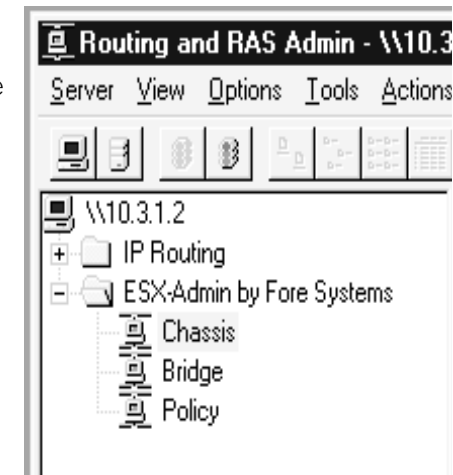
The system displays the tree view of the switch.

3. Open the IP Routing and the ESX-Admin by FORE Systems folders by clicking on the + icons.

The system displays the switch expanded tree view.

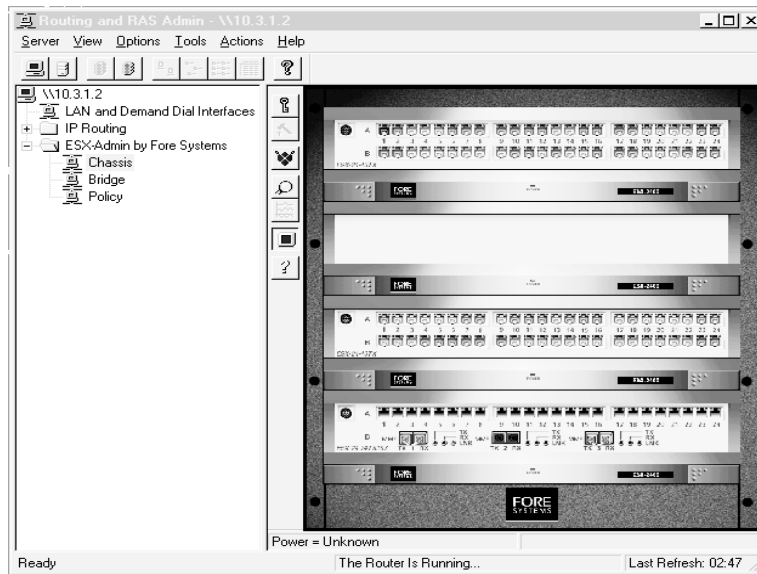


4. Click on the chassis icon. The chassis display will appear in the screen's display view (shown on the following page).



When the chassis view appears in the display view on your screen, it indicates you have completed Startup successfully.

Chassis View



Legend

Port Indicators

During configuration, you will notice that the ports on the chassis display will change color to indicate:

- Blue** NSC control port
- Green** Configured, and link established
- Yellow** Configured, and no link established
- White** Not configured, but link established
- Blank** Not configured, and no link established

Status Messages

During operation, status messages will appear at the bottom of the chassis display to indicate:

- Temperature
- System Status

Note: You can expand and shrink the size of the window using standard window sizing controls.

Go to Chapter 5, "Switch Configuration", and continue the process of configuring the switch in your network.

After you complete the Startup procedure, follow the instructions in this chapter and begin configuring your ESX Switch.

This chapter provides a configuration overview and contains instructions for configuring the chassis, line cards, and ports. It describes how to name a redundant NSC and how to save your configuration after you change the configuration. It also describes how to view chassis-related information that the switch maintains.

Chapter 5 contains the following sections:

- 5.1 Configuration Overview
- 5.2 Configure Chassis
- 5.3 Configure Line Cards
- 5.4 Customize Ports
- 5.5 Name Redundant NSC
- 5.6 View Port Information
- 5.7 View Chassis Information

After configuring the chassis, you can configure:

- Bridges – Chapter 6
- IP and Routing Protocols – Chapter 7
- Trunk Groups – Chapter 8

5.1 Configuration Overview

You can configure ports on the ESX Switch to operate in the following ways, as: bridged ports, as routed ports, and as multilayer switched ports (combination bridge/router).

In addition, you can configure multiple ports connecting two ESX switches as trunked ports, providing a high-bandwidth pathway between the switches.

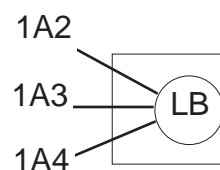
This section provides an overview of the following configuration options:

- Bridged Ports
- Routed Ports
- Multilayered Switched Ports
- Trunked Ports

Bridged Ports

Ports on the switch that you designate as members of a bridge group function as if they were all physically connected.

Diagram

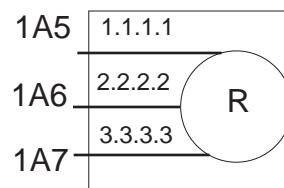


Action

1. Traffic coming for unknown destinations is flooded to all other ports in the bridge group.
2. Broadcast and multicast traffic is always flooded to all other ports in the bridge group.
3. Individual MAC addresses are learned as traffic is bridged between ports on the bridge group so that future traffic will be forwarded only to the port leading to specified destination.

Routed Ports

When you configure ports on the switch as IP ports and configure routing protocols (such as OSPF or RIP) on those



ports, they operate as follows:

Diagram

Action

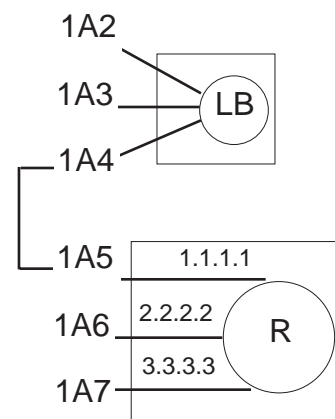
1. Routed ports consist of two or more IP subnets.
2. Only traffic addressed to a MAC address on the router's IP interface will be forwarded.

5.1 Configuration Overview (continued)

Multilayered Switched Ports

You can assign an IP address to a switch port and designate it as a member of a bridge group. Refer to the description that follows for port 4.

Diagram



Action

1. Ports 2 and 3 operate as bridged ports, described previously.
2. Ports 6 and 7 operate as routed ports, described in the previous section.
3. Port 5 acts like a routed port if it receives IP traffic with a MAC address = to the MAC address of its port. It bridges all other traffic it receives
4. Port 4 connects Port 5 to the Bridge Group.

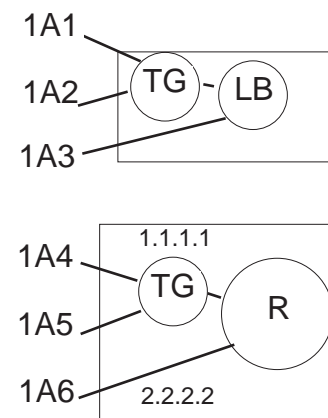
Trunked Ports

You can establish trunked ports, whether ports are routed or bridged, and once established, trunked ports operate similarly, regardless of whether they form part of a bridge or a router.

You can establish trunked ports to provide more bandwidth and establish a backup interface in the event a port connection fails.

The diagram shows trunks established on a learning bridge and on a router. When the switch receives frames from a group of trunked ports it treats the frames as if they were coming from a single port. Similarly, when the switch is sending, it balances the frame traffic among the trunked ports.

Diagram



Action

1. Ports 1 and 2 belong to a bridged trunk group.
2. Port 3 operates as a bridged port, described previously.
3. Ports 4 and 5 share a common IP address and belong to a routed trunk group.
4. Port 6 operates as a routed port, described previously.

5.2 Configure Chassis

Access the Chassis Configuration page to enter the serial number of the switch and other key system information. To access the Chassis Configuration page:

In Tree View

**Right Click
Chassis Icon**

**Select a Line
Card**

**Right Click to
Display Editing
Mode Popup**

**Select Editing
Mode**

**Right Click and
Select
Configure
Chassis**

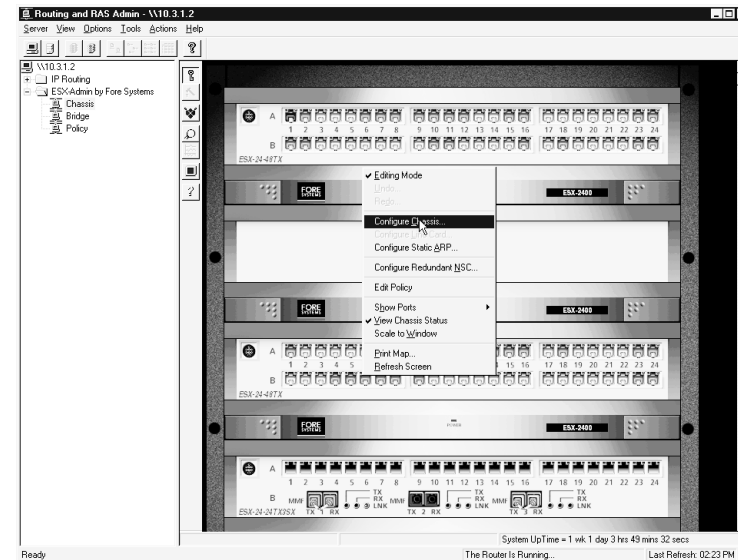
In the Tree View:

1. Select the Chassis icon, displaying a graphical representation of the chassis in the display view.
2. Select the line card you want to configure by clicking on it.
3. Right click to display the Editing Mode popup.

4. Select the Editing Mode item to display a check mark next to Editing Mode.

Note: When positioned in display mode, the cursor now appears as a key. Previously it appeared as a padlock.

5. Right click to display the Editing Mode popup again, and select Configure Chassis, displaying the Chassis Configuration page shown on the following page.



5.2 Configure Chassis (continued)

Enter the serial number of the switch and other key system information on the Chassis Configuration page:

On Chassis
Configuration
page

Modify Chassis
Configuration
page

On the Chassis Configuration page:

1. Enter data in the fields provided.

The screenshot shows a 'Chassis Configuration' window with two tabs: 'General' and 'Administration'. In the 'General' tab, there are three fields: 'Model Id' (a dropdown menu currently showing 'ESX-2400' with a list of options including 'ESX-4800', 'ESX-2400s', and 'ESX-NIC'), '32-bit Unique Id' (an empty text field), and 'Description' (an empty text field). In the 'Administration' tab, there are three text input fields: 'Contact' (containing 'Doug -- x2001'), 'Unit Name' (containing 'Gold'), and 'Unit Location' (containing 'Engineering Lab - Orofino'). At the bottom of the window are 'OK' and 'Cancel' buttons.

The example shows these chassis configuration parameters and values:

Parameter	Value
Model ID	ESX-4800 or ESX-2400
Unique ID	Serial number of the switch printed on the label attached to the front of ESX-4800 and ESX-2400 chassis and the back of single ESX-2400 switch modules installed directly in the rack.
Contact	Name and phone number of department or person in charge of the switch.
Unit name	Name of the switch.
Unit location	Building and room number.

FORE Systems ESX Switch Administrator's Guide 5-5

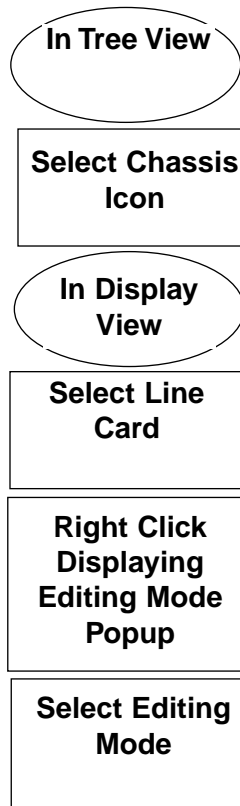
Note: The *unique ID* is printed on a bar-coded label attached to the:

- Front of an ESX-4800 Switch chassis.
- Front of an ESX-2400 Integrated Stack.
- Back of an ESX-2400 Switch module– use this number as the unique ID of the chassis when the switch module is installed in a rack, instead of in an ESX-2400 Integrated Stack.

5.3 Configure Line Cards

Access the Line Card Configuration page to define the line cards installed in your chassis. Configuring a line card is a two-step process: first, activate editing mode. Then select and configure a line card using the Line Card Configuration page.

To activate editing mode:



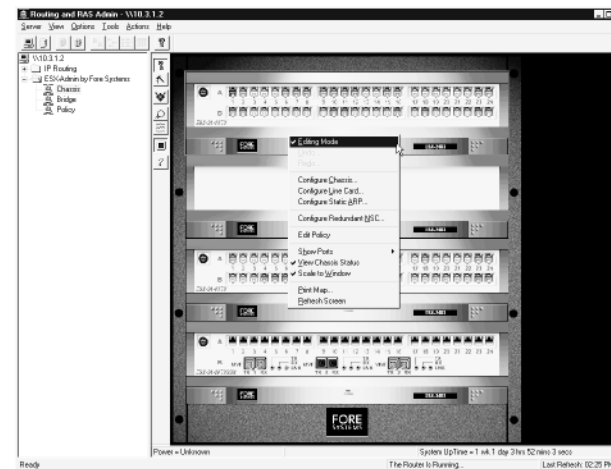
In the Tree View:

1. Select the Chassis Icon, displaying a graphical representation of the chassis in the display view.

In the Display View:

2. Select the line card you want to configure by clicking it.
3. Right-click to display the Editing Mode popup.
4. Select the Editing Mode item, displaying a check mark next to Editing Mode.

Note: When positioned in display mode, the cursor now appears as a key. Previously it appeared as a padlock.



5.3 Configure Line Cards (continued)

Continue configuring a line card by performing this procedure:

In Display View

Select a Line Card

**right-click
Displaying
Editing Mode
Popup**

**Select
Configure Line
Card**

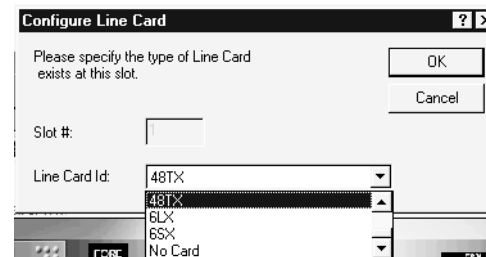
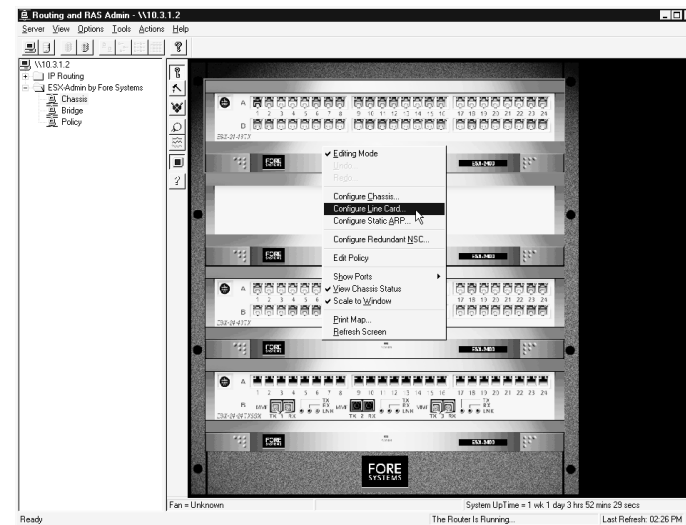
**Specify Line
Card Type**

Click OK

In the Display View:

1. Select a line card you want to configure by clicking on it.
2. Right-click to display the Editing Mode popup menu.
3. Select the Configure Line Card item in the Editing Mode popup menu to display the Configure Line Card page.
4. Specify the type of line card.
5. Click OK.

Note: Repeat steps 1 - 4 for each line card installed in the chassis.



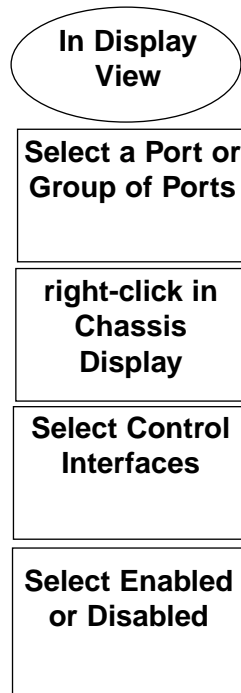
5.4 Configure Ports

Using ESX-Admin, you can configure the ports connected to the switch. This section describes how to select control ports—the ports that are configured to communicate with the NSC. And it describes how to set a port's Ethernet parameters manually. For information on how to perform these port-related tasks, refer to the following sections:

- Configure Control Interfaces
- Configure Ethernet Interfaces

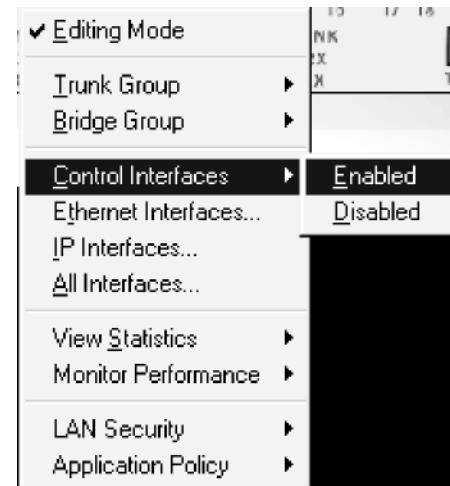
5.4.1 Configure Control Interfaces

Using ESX-Admin, you can configure the control interfaces on the switch. When you connect a cable between a port configured as a control interface and the NSC's adapter 1, the NSC and the switch communicate across this port. An interface that is defined as a control interface will become the control port when it is connected to the NSC's adapter 1.



In the Display View:

1. Select the port or group of ports to enable or disable as control interfaces.
2. Right-click to display the edit popup menu.
3. Select the Control Interfaces item, to display a submenu. (see example).
4. Select Enabled or Disabled.



5.4.2 Configure Ethernet Interfaces

By default, all ports on the switch autonegotiate to determine speed and mode. Access the Ethernet Port Configuration page to set Ethernet parameters to a specific setting for a port or group of ports.

Note: 10/100 Base TX and Gigabit ports operate differently.

- 10/100 Base TX ports, can be configured to operate at either 10 or 100 Mbit speeds and in full or half duplex modes. *This section describes how to manually configure 10/100 Base TX ports.*
- Gigabit ports can either autonegotiate or, if autonegotiation is disabled, they will operate at 1000 Mbit speed in full duplex mode. *Refer to the **ESX-Cli Command Console Guide** for information describing how to disable autonegotiation on gigabit ports.*

Use this procedure to manually set the speed of TX ports to 10Mbps or 100Mbps.

In Display View

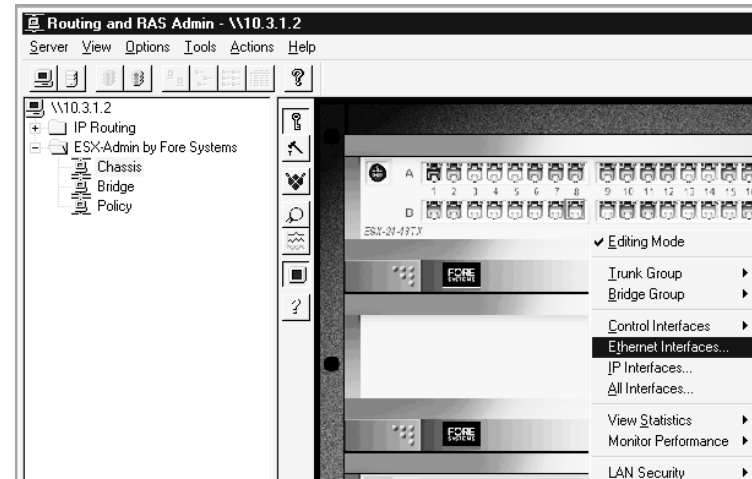
Select a Port

Right-Click in Chassis Display

Select Ethernet Interfaces

In the Display View:

1. Select a port or multiple ports to configure.
2. Right-click to display the edit popup menu.
3. Select the Ethernet Interfaces item to display the Ethernet Port configuration page



5.4.2 Configure Ethernet Interfaces (continued)

Note: Both link partners—local and remote devices—must be configured with compatible settings in order to establish a reliable link. If link partners are unable to communicate, verify that their settings are compatible.

To set speed and mode settings manually for 10/100 TX ports:

**On Ethernet
Port
Configuration
Page**

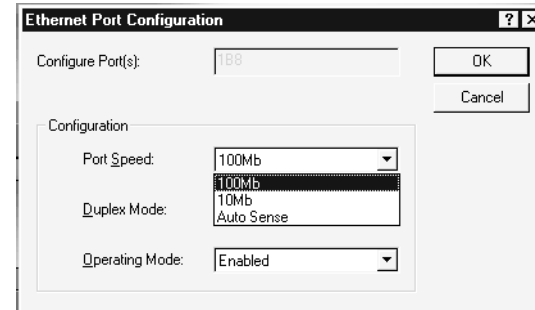
Set Port Speed

Set Mode

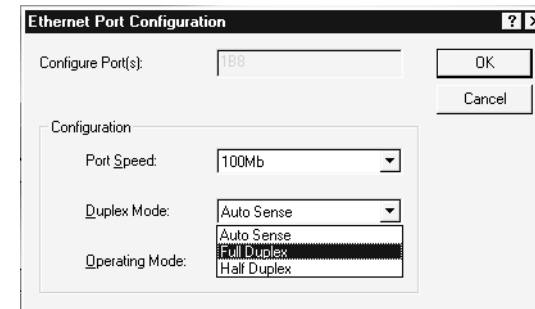
Click OK

On the Ethernet Port Configuration page:

1. Set port speed for a port or group of ports to 10 or 100 Mbit.
2. Set mode for a port or group of ports to full or half duplex.
3. Click OK.



See online help for details. Click the ? icon in the menu bar and click on a field to access online help.



5.5 Cold Standby

When you implement a cold standby configuration, you connect two NSCs to a single switch—specifying one NSC as a primary and the other NSC as a backup.

Note: Both NSCs are dedicated to the switch—you cannot connect either NSC to another switch.

If the primary NSC fails, the backup will load its configuration onto the switch and take control.

Note: The failover time will depend on the size and complexity of the configuration the backup NSC loads onto the switch when it assumes control.

5.5.1 Connecting the Two NSCs to the Switch

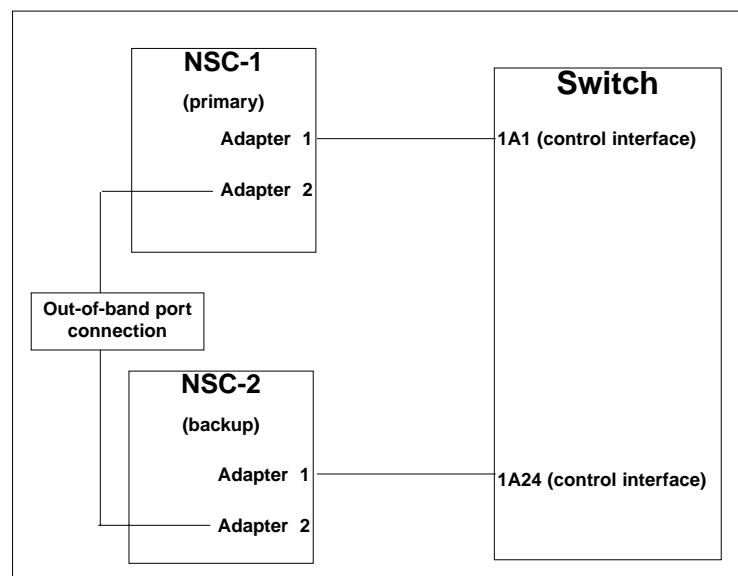
To configure cold standby, you will need to connect 2 NSCs to separate ports on the switch. The primary NSC will be the NSC that you connect to switch first. *See the following diagram.*

Note: You must configure the ports on the switch where the NSCs are attached as *control interfaces*. *See Section 5.4.1, “Configure Control Interfaces”.*

5.5.2 Connecting the Two NSCs Together

You also need to connect the primary and backup NSCs via an out-of-band connection. You can connect other machines on the same out-of-band link used by the primary and backup NSCs to communicate.

You can verify that the primary and backup NSCs can communicate with each other by having the primary NSC ping the backup NSC's out-of-band port. See the **ESX-Cli Command Console Guide** for details.



Cold Standby Configuration

5.5.3 Configuring the Backup NSC

You can configure a backup NSC, also called a redundant NSC, using ESX-Admin or ESX-Cli.

To configure a backup NSC using ESX-Admin:

In Tree View

Select Chassis
Icon

In Display
View

Right-click to
Display Edit
Menu and
Select Editing
Mode

Right-click and
Select
Configure
Redundant
NSC

Enter NSC
Names

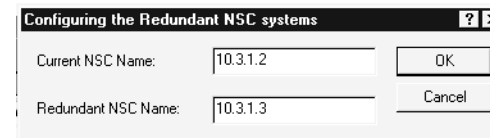
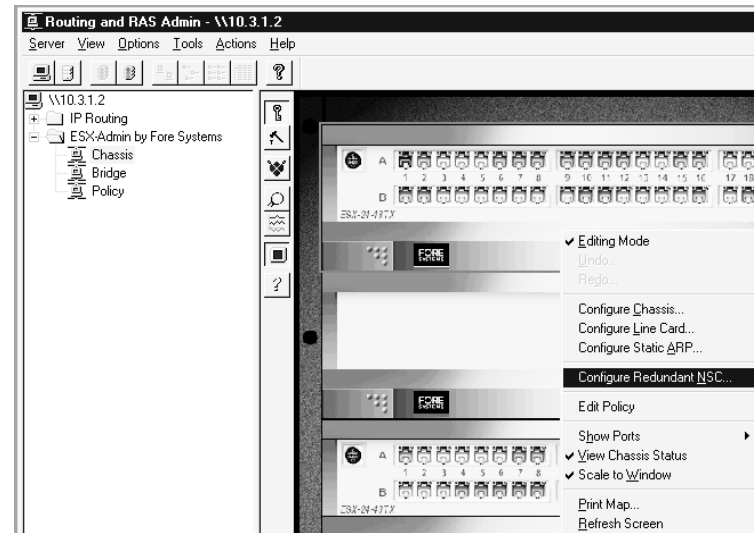
Click OK

In the Tree View:

1. Select the Chassis icon.

In the Display View:

2. Right-click to display the Edit Menu and select Editing Mode.
3. Right-click to display the Edit Menu again and select the Configure Redundant NSC item to display Configure the Redundant NSC systems page.
4. Enter the Current NSC name or IP address and the Redundant NSC name or IP address in the respective windows.
5. Click OK.



Note: To configure a backup NSC using ESX-Cli, issue the following ESX-Cli commands while you are connected to NSC-1:

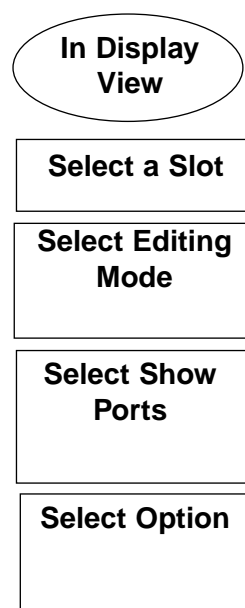
```
CLI> cfg nsc peer1 10.0.0.1 peer2 10.0.0.2
```

where: NSC-1 OOB = 10.0.0.1–primary
NSC-2 OOB = 10.0.0.2–secondary

5.6 View Port Information

You can view special port information in the chassis display. The chassis display shows the ports that are enabled for control information and the ports that belong to bridge groups. The chassis display also provides the status of individual ports. See Section 4.5, "Access the Chassis Display", for information on how colors are used to indicate port status.

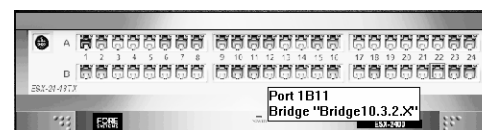
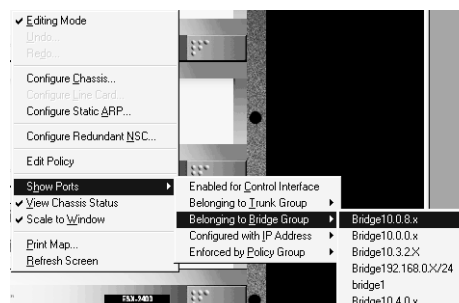
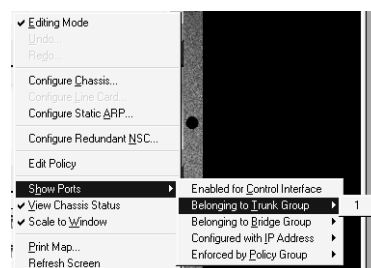
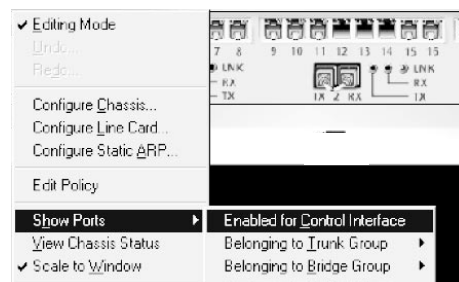
To view port information:



In the Display View:

1. Select a slot.
2. Right-click to display the Edit Menu, Select Edit Mode and right-click again to display Edit Menu with Edit Mode selected.
3. Select Show Ports.
4. Select either Enabled for Control Interface, Belonging to Trunk Group, or Belonging to Bridge Group

Note: The logical port number of the bridge and the bridge address appear in the popup. And a red outline highlights the members of the bridge group.



5.7 View Chassis Information

You can view chassis-related information in the chassis display, by selecting the View Chassis Status option on the edit menu.

In Display View

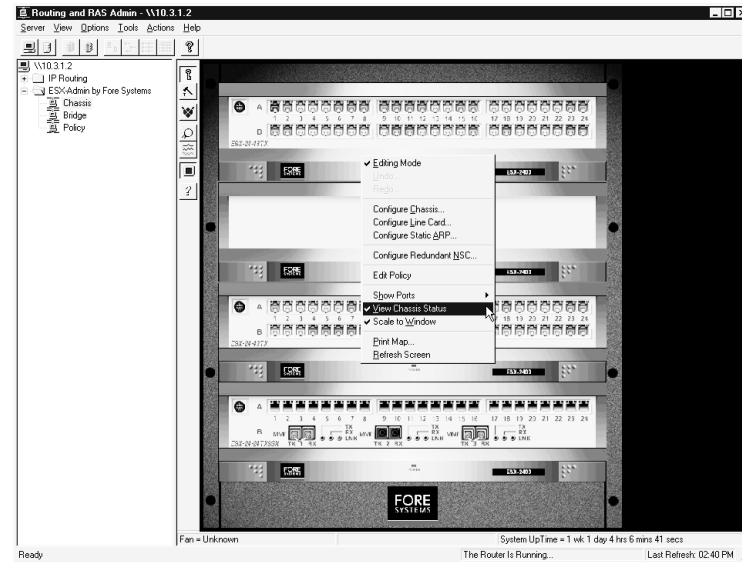
Select a Slot

Select Editing Mode

Select View Chassis Status

In the Display View:

1. Select a slot.
2. Right-click to display the Editing Mode popup; and select Editing Mode.
3. Right-click again to display Editing Mode popup with Editing Mode selected; and select the View Chassis Status item to display chassis messages at the bottom of the chassis view.



Note: Power, temperature, and switch status messages appear periodically at the bottom of the chassis display.

5.7 View Chassis Information (continued)

In addition to the chassis information displayed at the bottom of the screen, the system provides the following views of chassis-related information:

- Chassis Table
- Module Table
- LCP Table
- Ethernet Statistics Table

To view chassis information:

In Tree View

**Select Chassis
Icon**

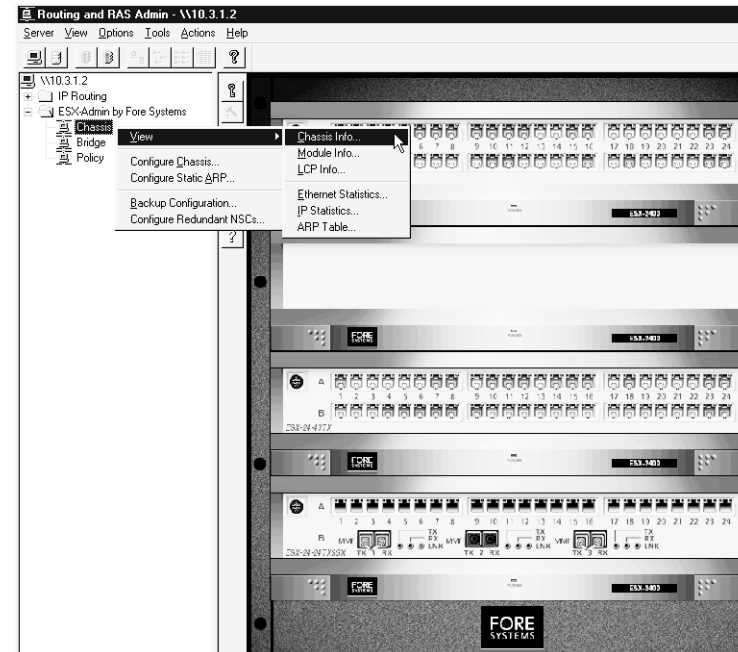
**Right-click to
Display Popup**

Select View

**Choose View
Selection from
Popup**

In the Tree View:

1. Select the Chassis icon.
2. Right-click to display a popup.
3. Select the View item and hold down the mouse to display a secondary popup listing view options.
4. Select the view you would like to display.



Chassis Table

Admin Name Switch administrator.

The Chassis Table shows these parameters:

Chassis										
Revision	Unique Id	Status	Maximum Sl...	Maximum P...	Power Status	Description	Admin Name	Unit Name	Unit Location	NSC Port
0	0	Normal Oper...	1	48	Unknown			nsc-chaak		1A1

<u>Parameter</u>	<u>Description</u>
------------------	--------------------

Revision	Revision number of the switch.
----------	--------------------------------

Unique ID	Unique identifier printed on a bar-coded label attached to the switch.
-----------	--

Status	Operational status of the switch.
--------	-----------------------------------

Maximum Slots	8 slots for an ESX-4800, 4 slots for an ESX-2400.
---------------	---

Maximum Ports	384 100 MBit ports for an ESX-4800, 192 for an ESX-2400.
---------------	--

Fan Status	Indicates whether fans are in normal operating range.
------------	---

Temperature	Indicates whether temperature is in normal operating range.
-------------	---

Description	Description of the switch.
-------------	----------------------------

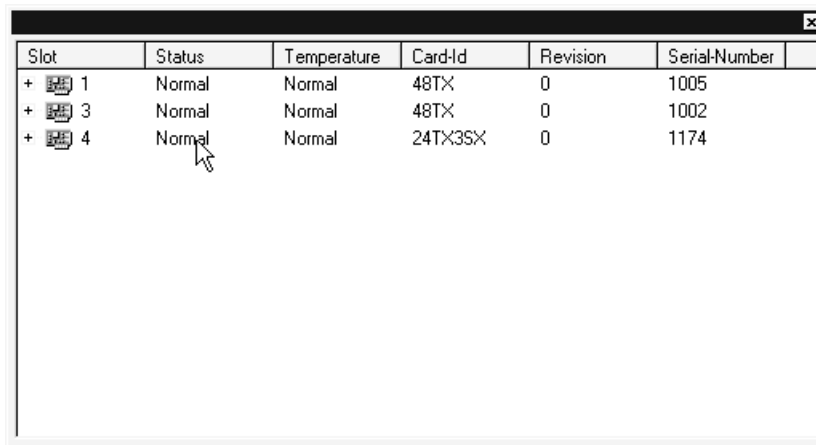
Unit Name	Switch name—up to 15 characters.
-----------	----------------------------------




Unit Location	Switch location.
---------------	------------------

Note: Right-click in the chassis display and select the Customize option to view more chassis parameters.

Module Table

The Module Table shows these parameters:

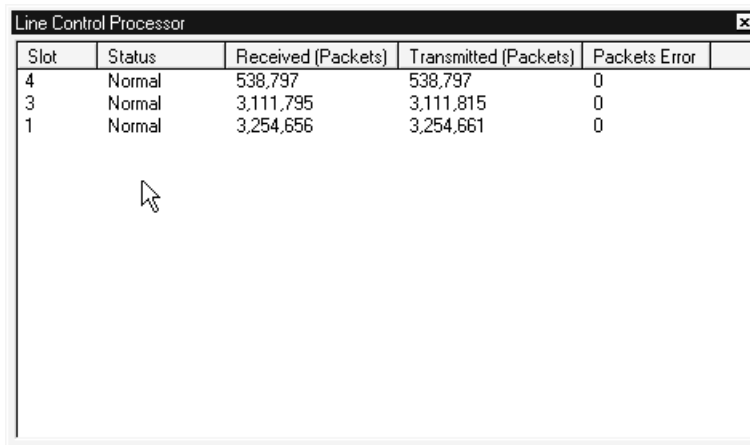


Slot	Status	Temperature	Card-Id	Revision	Serial-Number
+  1	Normal	Normal	48TX	0	1005
+  3	Normal	Normal	48TX	0	1002
+  4	Normal	Normal	24TX35X	0	1174

<u>Parameter</u>	<u>Description</u>
Slot #	Modules slot number—assigned by the switch.
Status	Operational status of the switch.
Temperature	Indicates whether temperature is in normal operating range.
Card ID #	Module type.
Revision #	Revision number of the switch.
Serial #	Unique identifier printed on a bar coded label attached to the switch.

Line Control Processor Table

The Line Control Processor Table shows these parameters:



Slot	Status	Received (Packets)	Transmitted (Packets)	Packets Error
4	Normal	538,797	538,797	0
3	Normal	3,111,795	3,111,815	0
1	Normal	3,254,656	3,254,661	0

<u>Parameter</u>	<u>Description</u>
Slot #	Slot location of the module.
Status	Operational status of the switch.
Received Packets	Packets received by this LCP.
Transmitted Packets	Packets sent by this LCP.
Packets Error	Packets received with errors.

Note: Right-click in the Line Control Processor display and select the Customize option to view more LCP parameters.

Ethernet Statistics Table

The Ethernet Statistics Table shows these parameters:

MAC Speed	Link State	Rcv Packets	Duplex Mode	Rcv Unkno...	Snd Packets	Rcv Octets	Rcv Unicast...	Rcv Non-un...	Rcv Unkno...	Rcv Discard...	Rcv Discard...	Snd
100 MB	Online	4.8148e+006	Full Duplex	0	4.4885e+006	3.4611e+009	0	0	0	1.5e+001	1.8784e+004	3.51
10 MB	Online	4.1254e+004	Half Duplex	0	6.8715e+004	5.2057e+007	0	0	0	4.1253e+004	5.2056e+007	2.39
100 MB	Online	3.088e+003	Half Duplex	0	6.9269e+004	3.1599e+005	0	0	0	5	3.9e+002	5.47
100 MB	Online	2.51e+002	Half Duplex	0	7.098e+004	3.4633e+004	0	0	0	0	0	5.49
100 MB	Online	4.32e+002	Half Duplex	0	7.0879e+004	6.0852e+004	0	0	0	5	3e+002	5.49
100 MB	Online	6.7979e+005	Half Duplex	0	2.2673e+004	5.2511e+008	0	0	0	5.6648e+005	4.3302e+008	4.03
100 MB	Online	5.54e+003	Full Duplex	0	7.5064e+004	1.5693e+006	0	0	0	0	0	5.65
Undefined	Offline	1	Auto Sense	0	0	1.6e+002	0	0	0	0	0	0
100 MB	Online	5.9372e+004	Half Duplex	0	1.6563e+006	5.4672e+007	0	0	0	5.9371e+004	5.4672e+007	1.30
100 MB	Online	8.456e+003	Full Duplex	0	9.5933e+004	2.4303e+006	0	0	0	9	1.067e+003	5.90
100 MB	Online	5.03e+002	Full Duplex	0	9.3364e+004	6.1997e+004	0	0	0	0	0	5.78
100 MB	Online	5.1381e+005	Full Duplex	0	6.002e+005	1.2897e+008	0	0	0	0	0	1.47
100 MB	Online	2.309e+006	Half Duplex	0	3.1722e+005	1.5764e+009	0	0	0	1.8681e+006	1.3234e+009	1.02
100 MB	Online	9.7007e+004	Half Duplex	0	1.8958e+005	5.922e+007	0	0	0	9	8.13e+002	8.33
Undefined	Offline	1	Auto Sense	0	0	1.6e+002	0	0	0	0	0	0

Parameter	Description
MAC Speed	Speed of the device attached to the interface.
Link State	Indicates if the link is active.
Rcv Packets	Packets received on this port.
Duplex Mode	Half Duplex or Full Duplex.
Rcv Unknown	Packets received with invalid destination address.
Snd Packets	Packets transmitted on this port.

Note: Right click in the Ethernet Statistics display to display a popup, then select the Customize option to view more Ethernet parameters. Select the Counter Display Format to define the numeric format for the statistics display.

Follow the instructions in this chapter to configure network equipment connected to ports on the switch as a bridge group. When you select ports on the switch and define them as members of a bridge group, the switch will relay frames between these ports as if they were separate network segments physically connected by a bridge.

Using the Bridge Creation Wizard or the ESX-Admin facility, you can configure the switch to function as a transparent bridge. Optionally, you can run the spanning tree protocol on the bridge group. This chapter contains the following sections that will guide you in configuring a bridge group:

- 6.1 Bridging Overview
- 6.2 Bridge Creation Wizard
- 6.3 Create a Transparent Bridge Group
- 6.4 Create a Spanning Tree Bridge Group
- 6.5 View Bridge Statistics

6.1 Bridging Overview

The following diagram provides an example of a bridge group. In the diagram, ports 2, 3, and 8 are members of a bridge group.

Note: You can connect devices to the ports that you designate as members of the bridge group either before or after you configure the bridge group.

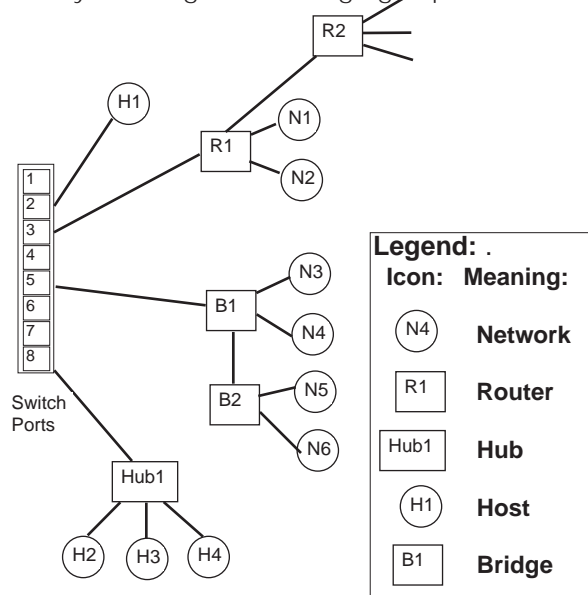


Diagram of a Sample Bridge Group

This chapter uses the sample bridge group diagram to illustrate how to configure a transparent bridge group and run the spanning tree protocol.

Glossary

Bridge A communication device that connects two or more networks and selectively forwards packets between them using the physical layer (layer 2 in the OSI model)

Bridges store and forward complete packets, *unlike repeaters that forward all electrical signals.*

Bridges use physical addresses, *unlike routers that use IP addresses.*

Bridge Group A logical bridge created by connecting network devices and hosts to ports configured as members of the bridge group.

Host Any end-user computer that connects to a network.

Hub A device to which multiple computers attach, often with twisted pair wiring. A hub simulates a network that interconnects the attached computers.

Network An arrangement of devices that are interconnected and the transmission channels that provide this interconnection.

Router A computer that connects to two or more local area networks and forwards layer 3 datagrams from one to another. Using the destination address in the datagram, the router picks the next hop and forwards the datagram.

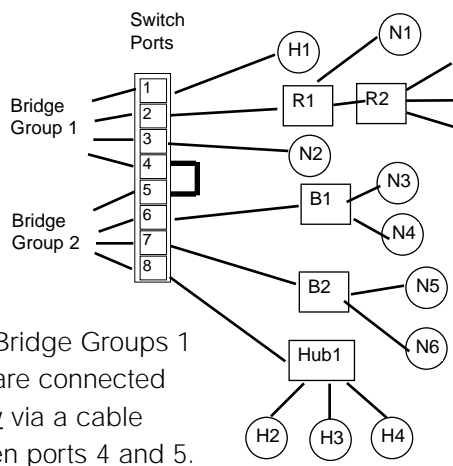
Caution: Avoid Interconnecting Bridge Groups

Bridge groups are independent layer 2 networks. Do not interconnect bridge groups or a loss of connectivity may result.

- Avoid connecting bridge groups, directly, using a cable.
- Also, avoid connecting bridge groups, indirectly, by connecting two ports on a bridge or a router to different bridge groups.

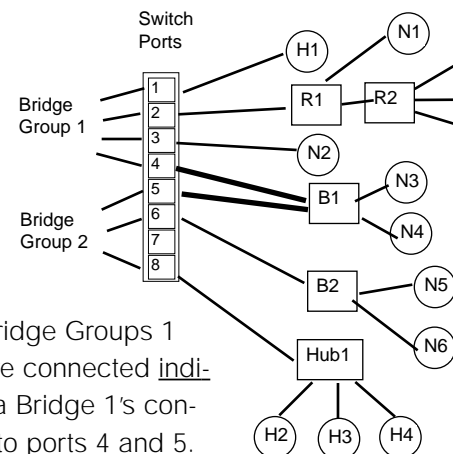
The following diagrams show the types of connections to avoid:

- Direct connection between bridge groups
- Indirect connection between bridge groups.



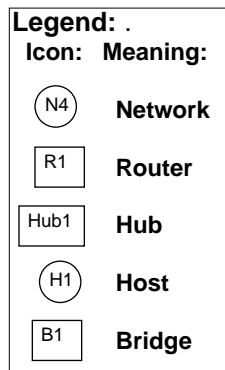
Note: Bridge Groups 1 and 2 are connected directly via a cable between ports 4 and 5.

Direct Connection between Bridge Groups



Note: Bridge Groups 1 and 2 are connected indirectly via Bridge 1's connection to ports 4 and 5.

Indirect Connection between Bridge Groups



Transparent Bridge

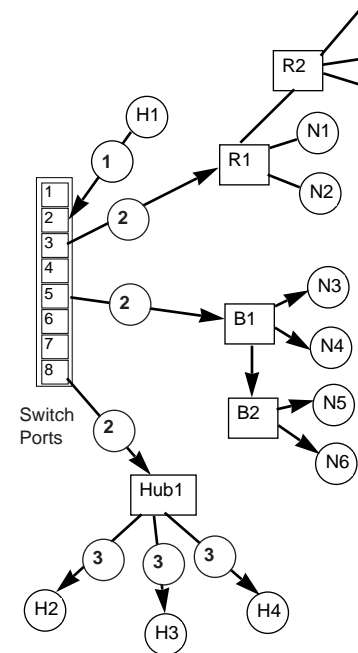
When configured as a transparent bridge, the switch performs these basic bridge functions:

- It receives packets and queues them for forwarding.
- It learns station locations by listening to packet traffic.
- If the destination end station's location is known, it forwards the packet to the port to which it is connected and not to other ports.
- If the destination end station's location is unknown, it floods the packet to all ports except the sending port.
- It performs CRC Checking.

Transparent Bridging Example

1. A *source host*, H1 attached to port 2, sends a packet to a *destination host*, H2 on Hub1.
2. If the bridge has never heard from the destination before, then the switch floods the packet to all active ports except the sending port—ports 3, 5, and 8. The switch learns the *sending host*, H1 with MAC address H1MAC resides on port 2 and notes this information in its learned table.
3. The destination host, H2, receives the packet via port 8 from Hub1.
4. The switch listens to the reply packet sent from the destination host, H2, to the source host and records its MAC address and its location, port 8, in its learned table.

5. Subsequent packets addressed to H2 are sent to port 8, rather than flooded to all ports.

**Transparent Bridging Example**

Spanning Tree Bridge

When configured to run the spanning tree protocol, the switch performs the same transparent bridging functions described in the previous section. In addition, it eliminates loops by:

- Dynamically configuring a “tree”—a subset of the network topology that is loop-free
- Forwarding packets only to those ports that are part of the tree, thus eliminating loops. (Ports that are not part of the tree are held in a “blocked” state. They can be placed in a “forwarding” state later if components fail, are removed, or added.)

The bridges in the bridge group transmit configuration messages to each other so they can:

- Elect a root bridge
- Calculate the distance to the root bridge
- Choose a root port—the shortest path to the root bridge
- Select a designated bridge for each LAN
- Select ports that make up the spanning tree.

Spanning Tree Scenario

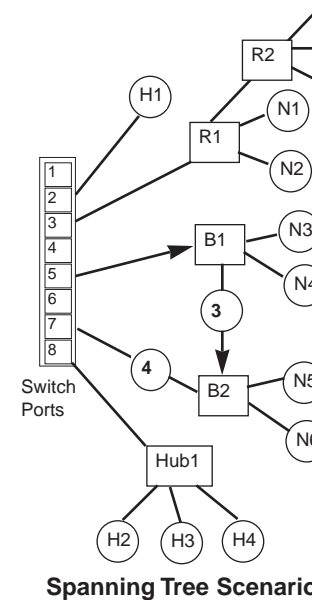
1. Two interconnected bridges (B1 and B2) connect to the switch, via ports 5 and 7, creating the potential for a loop to occur.

2. Unless a spanning tree is configured, a loop is created when the switch broadcasts a frame to B1 on port 5 and B2 on port 7:

When B1 receives the frame on port 5, it forwards the frame to B2. B2 forwards the frame to the switch, and the switch sends the frame to B1 on port 5, creating a loop. Meanwhile, when B2 receives the initial frame on port 7, it forwards the frame to B1. B1 forwards the frame to the switch and the switch sends the frame to B2 on port 7, creating a second loop.

3. The spanning tree algorithm can break the loop by only sending packets to B2 through B1, thus blocking B2's connection to the switch on port 7.

Note: Port 7 can be activated if B2's connection to B1 fails, or if B1's connection to the switch via port 5 goes down. In the latter case, the switch can communicate with B1 through its connection to B2.



6.2 Bridge Creation Wizard

You can create a transparent bridge and configure the spanning tree protocol on the bridge group by following step-by-step instructions in the Bridge Creation Wizard. Access the Bridge Creation Wizard from the tree view:

In Tree View

**Right Click
Bridge Icon**

**Select Use
Bridge Creation
Wizard**

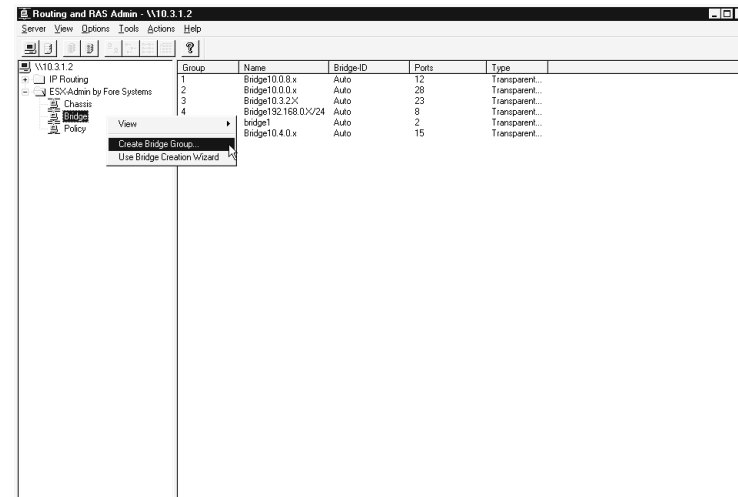
**Right Click
Bridge Icon**

**Select Create
Bridge Group**

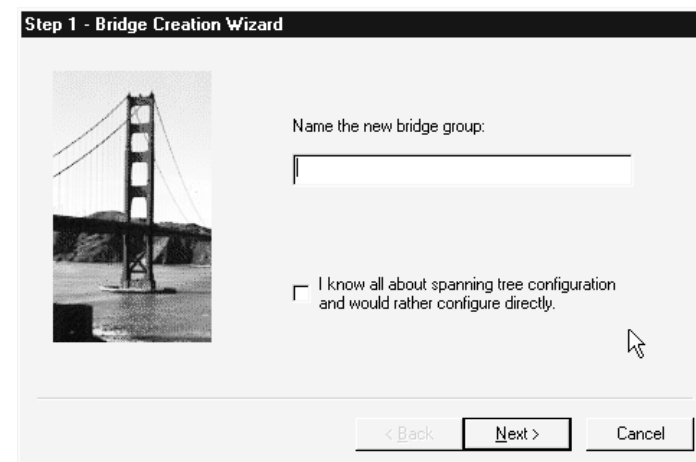
**Follow
Wizard
Instructions**

In the Tree View:

1. Right-click on the Bridge Icon displaying a pop-up menu.
2. Select the Bridge Creation Wizard item on the menu to place a check mark to the left of the item. (The menu will disappear.)
3. Right-click on the Bridge icon to display the Bridge Menu again.
4. Select the Create Bridge Group item on the menu to start the Wizard.
5. Follow instructions in the Wizard to configure Bridge ports.



The Wizard prompts you to name the new bridge group and gives you the option of configuring spanning tree directly or with the Wizard.



6.3 Create Transparent Bridge Group

To create a Transparent Bridge Group, access the Create Bridge Group page from the tree view or the chassis display.

In Tree View

**Select the
Bridge Icon**

**Right-Click to
Display Bridge
Menu**

**Select Create
Bridge Group**

**Modify Create
Bridge Group
Page**

In the Tree View:

1. Select the Bridge icon.
2. Right-click to display the Bridge menu
3. Select the Create Bridge group item to display the Create Bridge Group page.
4. Modify the Create Bridge Group page (described in the next section).

In Chassis Display

Select Ports

**Right Click in
Chassis
Display**

**Select Create
Bridge Group
item**

**Modify Create
Bridge Group
Page**

In the Display View:

1. Select user ports you want to configure as a bridge group.
2. Right-click to display the Editing Mode menu and highlight the Editing Mode menu item. A lock icon will appear next to the mouse pointer.
3. Right-click again to display the Editing Mode menu and select the Create Bridge Group item, to display the Create Bridge Group page.
4. Modify the Create Bridge Group page (described in the next section).

Specify Ports Belonging to the Bridge Group

Create the Transparent bridge group by defining values for the parameters on the Create Bridge page.

**On Create
Bridge
Group Page**

**Modify Create
Bridge Group
Tab Page**

Click Save

Click OK

On the Create Bridge Group page:

1. Fill in the bridge parameters (see example).
2. Add ports to the Bridge Group:
 - Select ports from the available Port ID list
 - Click Add to place them on the Bridge Ports list
3. Click Save.
4. Click OK.

The example shows these bridge parameters and values:

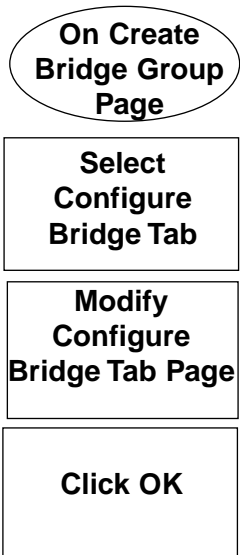
<u>Parameter</u>	<u>Value</u>
Name	Usually, department or region
Bridge Address	The bridge's Media Access Control (MAC) address, a 6 octet number Note: The MAC address must be unique on the network
Type	Transparent Only is supported

<u>Parameter</u>	<u>Value</u>
Available Port Id	List of available ports on the switch that can be part of the bridge
Bridge Ports	Ports you have assigned to the bridge group
Spanning Tree	Checking the box selects Spanning Tree protocol and displays two additional tabs at the top of the page (Spanning Tree configuration is described in the next section)

6.4 Configure Spanning Tree Protocol

Access the Configure Bridge tab page to configure the Spanning Tree protocol for the Root Bridge.

Note: If the bridge you are configuring becomes the Root Bridge, these values will apply to all the bridges in the spanning tree.



On the Create Bridge Group page:

1. Select the Configure Bridge tab to display the Configure Bridge tab page.
2. Select a parameter and modify it.

OR

Click the Use Default button to select the values that appear on the menu.

Note: The example shows the default values.

3. Click OK.

The example shows default Spanning Tree parameter values:

<u>Parameter</u>	<u>Value</u>
Bridge Max Age	The time bridges will wait without hearing hello messages before selecting a new root bridge. Information is discarded when this timer expires (range 6 - 40 seconds)

<u>Parameter</u>	<u>Value</u>
Bridge Hello Time	The time this bridge waits if it becomes the root bridge before sending a new hello message to the designated bridge on each LAN (range 1 - 10 seconds) Note: Designated bridges send hello messages downstream
Bridge Forward Delay	The length of time bridges spend in the "listening" state and in the "learning" state (range 4 - 30 seconds)

Configure Ports in a Spanning Tree Bridge Group
Access the Configure Ports tab page to set parameters for the ports that are members of the Spanning Tree.

**On Create
Bridge Group
Page**

**Select
Configure Ports
Tab**

**Modify
Configure Ports
Tab Page**

Click Save

Click OK

On the Create Bridge Group page:

1. Select the Configure Ports tab to display the Configure Ports tab page.
2. Select a port in the Port Id: list and configure it (see example).
3. Click Save.
4. Click OK.

The example shows bridge parameters and default values:

<u>Parameter</u>	<u>Value</u>
Port Path Cost	Cost associated with using a particular speed link: <ul style="list-style-type: none"> • 10Mbit link = 100 • 100Mbit link = 10 • 1000Mbit link = 1

<u>Parameter</u>	<u>Value</u>
Port Priority	The port priority parameter allows the network manager to prioritize the ports, other than by port number
Port Status	Enable or disable the port. A port can participate in frame relay only if it is enabled

6.5 Viewing Bridging Information

When you configure Transparent Bridge Groups and the Spanning Tree Protocol on your switch, you can view the information that the switch collects. The system provides the following information for viewing:

- Spanning Tree Information
- Spanning Tree Port Table
- Transparent Bridge Global Information
- Transparent Bridge Port Table
- Transparent Bridge Forwarding Database Table

The following sections provide samples of the information you can view:

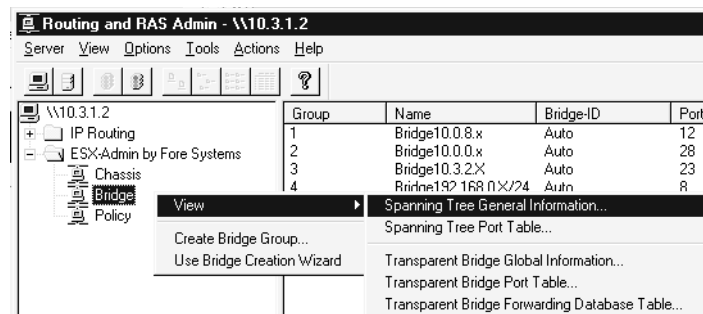
In Tree View

**Right Click
Bridge Icon**

**Select View
and the
Information You
Want to View**

In the Tree View:

1. Right-click the bridge icon to display the popup menu.
2. Select the View item on the menu to display the list of bridge information you can view, then select the item you want to view.



Spanning Tree Information

When you select Spanning Tree Information on the view sub-menu, the switch will display a table looking similar to this:

Spanning Tree Information												
Bridge Group	Priority	Root Id	Root Cost	Root Port	Max Age	Hello Time	Hold Time	Forward Delay	Bridge Max ...	Bridge Hello...	Bridge Forw...	
1	32768	80-00-00-E0...	0	0	20	2	1	15	20	2	15	
2	32768	80-00-00-E0...	0	0	20	2	1	15	20	2	15	
3	32768	80-00-00-E0...	0	0	20	2	1	15	20	2	15	
4	32768	80-00-00-E0...	0	0	20	2	1	15	20	2	15	

The example shows bridge parameters and values:

Parameter	Value
-----------	-------

Bridge Group	Number of the bridge group on the switch.
--------------	---

Priority	The relative priority of the bridge within the set of bridges in the bridge group (range 0-65535).
----------	--

Root Id	MAC address of the Root Bridge.
---------	---------------------------------

Root Cost	Cost of the path to the root as seen from this transmitting bridge (can be set for each port).
-----------	--

Root Port	The port number of the port offering the lowest cost path from this bridge to the root bridge.
-----------	--

Max Age	The length of time a bridge will wait without hearing hello messages before selecting a new root bridge. Information is discarded when this timer expires (range 6 -40 seconds).
---------	--

Hello Time	The time the root bridge waits before sending a new hello message to the designated bridge on each LAN. Designated bridges forward hello messages downstream (range 1 - 10 seconds).
------------	--

Hold Time	The interval of time during which no more than two configuration messages will be transmitted.
-----------	--

Forward Delay	The length of time spent in the "listening" state and in the "learning" state (range 4 - 30 seconds).
---------------	---

Spanning Tree Port Table

When you select Spanning Tree Port Table on the view sub-menu, the switch will display a table looking similar to this:

Port ...	State	Status	Path Cost	Received TCNs	Transmitted TCNs
1A3	Forwarding	Enabled	10	0	0
1A4	Forwarding	Enabled	10	0	0
1A5	Forwarding	Enabled	10	0	0
1A6	Forwarding	Enabled	10	0	0
1A7	Forwarding	Enabled	10	0	0
1A8	Disabled	Enabled	10	0	0
1A10	Forwarding	Enabled	10	0	0
1A11	Forwarding	Enabled	10	0	0
1A12	Forwarding	Enabled	10	0	0
1A13	Forwarding	Enabled	10	0	0
1A14	Forwarding	Enabled	10	0	0
1A15	Disabled	Enabled	10	0	0

The example shows bridge parameters and values:

Parameter Value

Port Physical port number on the switch, where
2=Slot number, A=Media, 1=connector
number.

State The current state of the port, either: disabled,
blocking, listening, learning, forwarding, or
broken.

Status The current status of the port, either:
enabled, capable of forwarding frames, or
disabled, incapable of forwarding frames.

Path Cost

The cost added to the root path cost when
calculating the cost to reach the root through
this port.

Received T...

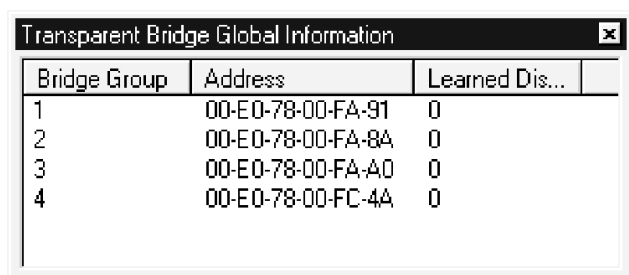
Received TCNs (Topology Change
Notifications).

Transmitted..

Transmitted TCNs (Topology Change
Notifications).

Transparent Bridge Global Information

When you select Transparent Bridge Global Information on the view submenu, the switch will display a table looking similar to this:



Bridge Group	Address	Learned Dis...	
1	00-E0-78-00-FA-91	0	
2	00-E0-78-00-FA-8A	0	
3	00-E0-78-00-FA-A0	0	
4	00-E0-78-00-FC-4A	0	

The example shows bridge parameters and values:

<u>Parameter</u>	<u>Value</u>
Bridge Group	The number of the bridge group that you configured on the switch.
Learned Dis...	The total number of Forwarding Database entries that were learned but were discarded because of lack of space in the database.

Transparent Bridge Port Table

When you select Transparent Bridge Port Table on the view submenu, the switch will display a table looking similar to this:

Transparent Bridge Port Table							
Max Info	In Frames	Out Frames	In Discards	In Octets	Port Number	Out Octets	Inbound Dis...
0	2.355e+003	9.657e+003	0	2.4482e+005	1A3	5.5054e+005	0
0	2.55e+002	1.1683e+004	0	3.388e+004	1A4	1.3596e+006	0
0	4.81e+002	1.1873e+004	0	6.6726e+004	1A5	1.3941e+006	0
0	8.4068e+004	2.4451e+004	0	6.9792e+007	1A6	4.6245e+006	0
0	5.434e+003	1.633e+004	0	1.5624e+006	1A7	2.9915e+006	0
0	0	0	0	0	1A8	0	0
0	7.596e+003	3.0706e+004	0	2.3362e+006	1A10	7.9829e+006	0
0	5.53e+002	2.8423e+004	0	6.8204e+004	1A11	7.5066e+006	0
0	6.8455e+005	7.0653e+005	0	1.6559e+008	1A12	1.2285e+008	0
0	5.3259e+005	4.1649e+005	0	3.3699e+008	1A13	1.2794e+008	0
0	1.1793e+005	1.4942e+005	0	7.0573e+007	1A14	3.8405e+007	0
0	0	0	0	0	1A15	0	0
0	4.2934e+005	5.6495e+005	0	1.9821e+008	1B1	2.6719e+008	0
0	0	0	0	0	1B2	0	0
0	0	0	0	0	1B3	0	0
0	0	0	0	0	1B4	0	0
0	0	0	0	0	1B5	0	0

The example shows bridge parameters and values:

Parameter	Value
-----------	-------

Port Number	Physical port number on the switch, where 1=Slot number, A=Media, 1=connector number.
-------------	---

Logical Port	The sequential number of the port, numbering from the first port on the switch.
--------------	---

Max Info	The maximum size of the INFO field that this port will receive or transmit.
----------	---

In Frames	The number of frames this port received from its segment.
-----------	---

Out Frames	The number of frames this port transmitted to its segment.
------------	--

In Discards	The number of valid frames that were received, but discarded by the forwarding process.
-------------	---

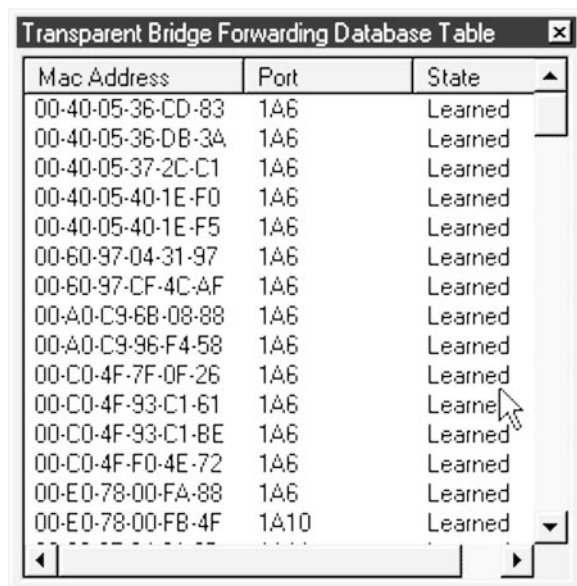
In Octets	Number of inbound 8-bit bytes received.
-----------	---

Out Octets	Number of outbound 8-bit bytes sent.
------------	--------------------------------------

Inbound Dis...	Number of discarded octets.
----------------	-----------------------------

Transparent Bridge Forwarding Database Table

When you select Transparent Bridge Port Table on the view submenu, the switch will display a table looking similar to this:



Mac Address	Port	State
00-40-05-36-CD-83	1A6	Learned
00-40-05-36-DB-3A	1A6	Learned
00-40-05-37-2C-C1	1A6	Learned
00-40-05-40-1E-F0	1A6	Learned
00-40-05-40-1E-F5	1A6	Learned
00-60-97-04-31-97	1A6	Learned
00-60-97-CF-4C-AF	1A6	Learned
00-A0-C9-6B-08-88	1A6	Learned
00-A0-C9-96-F4-58	1A6	Learned
00-C0-4F-7F-0F-26	1A6	Learned
00-C0-4F-93-C1-61	1A6	Learned
00-C0-4F-93-C1-8E	1A6	Learned
00-C0-4F-F0-4E-72	1A6	Learned
00-E0-78-00-FA-88	1A6	Learned
00-E0-78-00-FB-4F	1A10	Learned

The example shows bridge parameters and values:

<u>Parameter</u>	<u>Value</u>
MAC Address	Destination MAC address in a frame to which this entry's filtering information applies
Port Number	Physical port number on the switch, where 2=Slot number, A=Media, 1=connector number
State	The status of the table entry.

After Startup is complete, follow the instructions in this chapter to configure IP routing on your ESX Switch.

When configured for IP routing, the switch supports two methods of populating the IP routing table, either through statically configuring routes or by acquiring routing information via one of the supported dynamic routing protocols.

Two routing protocols are supported: Open Shortest Path First (OSPF) and Routing Information Protocol (RIP). Both OSPF and RIP can be configured on the same switch interface.

Configuring IP Routing consists of these sections:

- 7.1 Configuring IP Routing
- 7.2 Configuring OSPF
- 7.3 Configuring RIP
- 7.4 Configuring Static Routes
- 7.5 Configuring DHCP

7.1 Configuring IP Routing

To perform IP routing on the switch, you must configure the switch itself and those interfaces on the switch that will perform IP routing. This configuration must be performed before configuring routing protocols, such as OSPF and RIP, or assigning static routes to an interface. This section describes how to configure the switch and switch interfaces to perform IP routing:

Task

- Assign IP addresses to ports
- Configure IP parameters
- Configure interfaces
- Configure a static ARP entry
- View TCP/IP information
- View IP statistics

7.1 Configuring IP Routing

Chapter 7 Configuring IP Routing and Protocols

7.1.1 Assign IP Addresses to Ports

Before a port can communicate using the IP protocol, it must have an IP address. Perform this three-part procedure to assign an IP address to a port:

1. Select a port to configure
2. Access the IP Configuration page
3. Set the port's IP address and mask

To select a port to configure:

In Tree View

**Click ESX-
Admin by
FORE
Systems**

**Select
Chassis Icon**

**In Display
View**

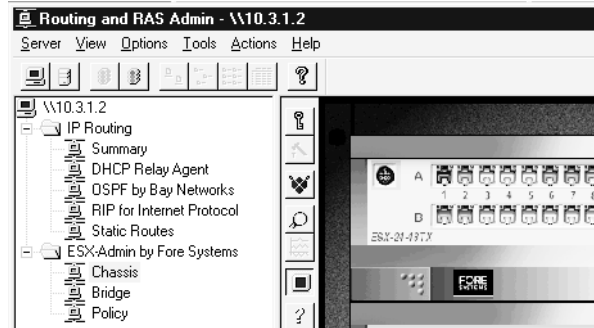
Select a Port

In the Tree View:

1. Click on the ESX-Admin by FORE Systems check box to display the Chassis icon.
2. Select the Chassis icon to show the chassis diagram in the display view.

In the Display View:

3. Select (highlight) a port or multiple ports on the chassis diagram that you would like to configure for IP routing.



7.1 Configuring IP Routing

Chapter 7 Configuring IP Routing and Protocols

7.1.1 Assign IP Addresses to Ports (continued)

Continue the procedure of assigning an IP address to a port, using the IP configuration page.

**In Display
View**

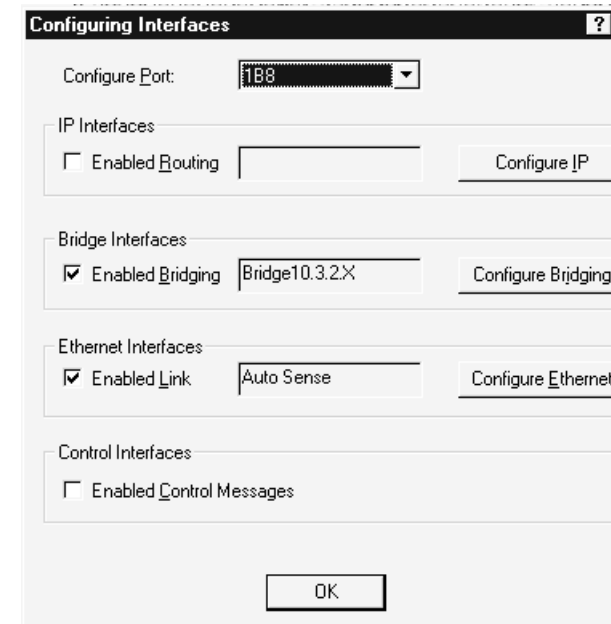
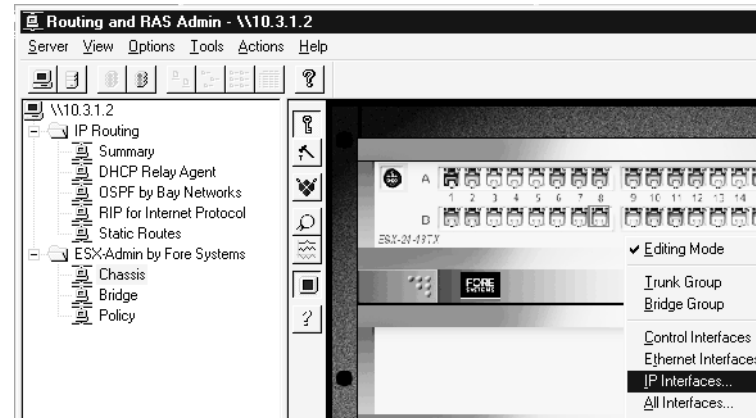
**Right-Click in
Display View**

**Select
Configure IP
Address**

In the Display View:

1. Right-click to display the Edit Mode pop-up menu.
2. Select the IP Interfaces menu item to display the IP Configuration page.

Note: You can also display the IP Configuration page by selecting the All Interfaces item on the menu, displaying the Configuring Interfaces screen, and clicking the Configure IP button.



7.1.1 Assign IP Addresses to Ports (continued)

Fill in the port IP address and mask on the IP Configuration page, completing the procedure of assigning an IP address to a port.

On IP Configuration Page

Assign IP Address and Mask

Click OK

On the IP Configuration page:

- 1. Assign an IP address and mask to the port.
- 2. Click OK.

Note: Repeat this procedure to configure additional ports.

The screenshot shows a dialog box titled "IP Configuration". It has three main sections: "Assign To", "IP Address", and "Operating Mode". In the "Assign To" section, the "Port" dropdown is set to "1A9". In the "IP Address" section, the "IP Address" field is "10 . 4 . 0 . 1" and the "Mask" field is "255 . 255 . 255 . 0". Below the mask field is a slider bar. In the "Operating Mode" section, the dropdown is set to "Enabled". On the right side of the dialog, there are three buttons: "OK", "Cancel", and "Delete".

The example shows these IP address parameters and values:

Parameter	Value
Port Number	Port number on the switch.
IP Address	Dotted decimal number, indicating the IP address associated with this switch port. The switch only supports assigning valid IP addresses to switch ports in the unicast address range: 0.0.0.0 - 223.255.255.255.
Mask	Bit mask used to indicate which bits in the IP address identify the link. Note: only contiguous masks are supported. You can generate a contiguous mask by moving the slider bar, located below the mask value.

7.1 Configuring IP Routing

Chapter 7 Configuring IP Routing and Protocols

7.1.2 Configure IP Parameters

When you configure IP parameters, you control how the switch will filter packets, log events and prioritize routes learned from each routing protocol. Perform this three-part procedure to configure IP parameters:

- Access the IP Configuration page
- Enable Packet Filtering and Event Logging
- Set Route Preferences

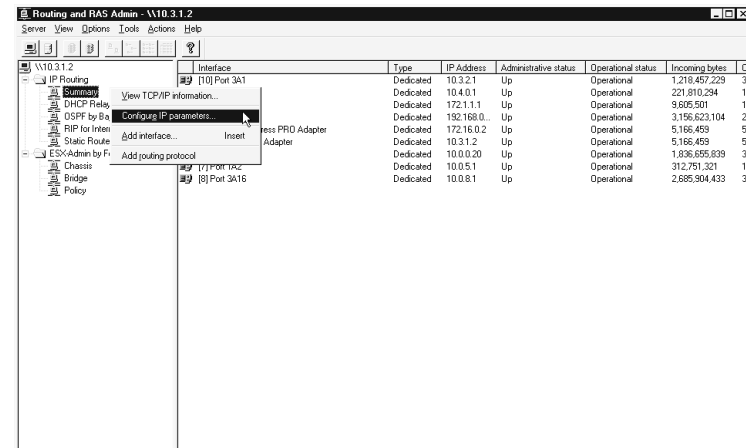
In Display View

Right-Click in Display View

Select Configure IP Parameters

In the Display View:

1. Right-click to display the Edit Mode pop-up menu.
2. Select the IP Interfaces menu item to display an IP Configuration page—see the following page.



Interface	Type	IP Address	Administrative status	Operational status	Incoming bytes	Outgoing bytes
[10] Port 3A1	Dedicated	10.3.2.1	Up	Operational	1,210,457,229	3
	Dedicated	10.4.0.1	Up	Operational	221,810,294	1
	Dedicated	172.1.1.1	Up	Operational	9,605,501	14
	Dedicated	192.168.0.1	Up	Operational	3,156,623,104	2
	Dedicated	172.16.0.2	Up	Operational	5,186,499	5
	Dedicated	10.3.1.2	Up	Operational	5,186,499	5
	Dedicated	10.0.0.20	Up	Operational	1,836,655,839	3
	Dedicated	10.0.5.1	Up	Operational	312,751,321	1
	Dedicated	10.0.8.1	Up	Operational	2,685,904,433	3

7.1 Configuring IP Routing

Chapter 7 Configuring IP Routing and Protocols

Enable Packet Filtering and Event Logging

To enable packet filtering and event logging perform this procedure:

**On General
Tab Page**

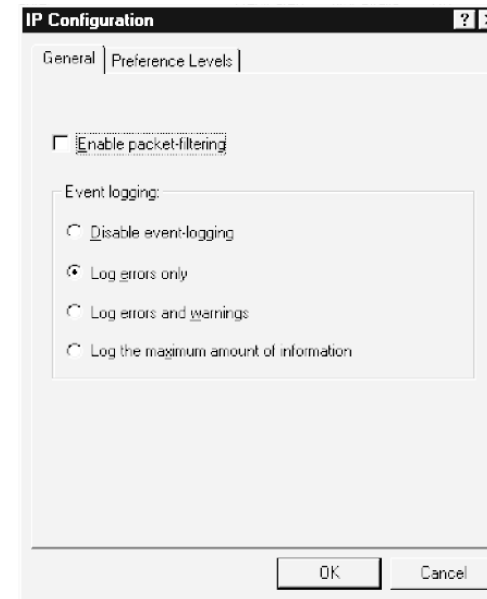
**Enable Packet
Filtering
(see caution)**

**Set Event
Logging
Preferences**

Click OK

On the General tab page:

1. Select Enable packet filtering check box.
2. Click the radio button to select the Event logging option.
3. Click OK.



Parameter	Value
Enable packet filters	When selected, enables packet filtering for any packets that must be forwarded by NT; it does <u>not</u> enable packet filtering for packets that pass between ports on the switch.
Event Logging	Click the ? icon in the menu bar and click on a field to access online help for event logging options. Note: When debugging, use the log the maximum amount of information setting.

Set Route Preferences

To set route preferences, perform this procedure:

**On
Preference
Levels Tab
Page**

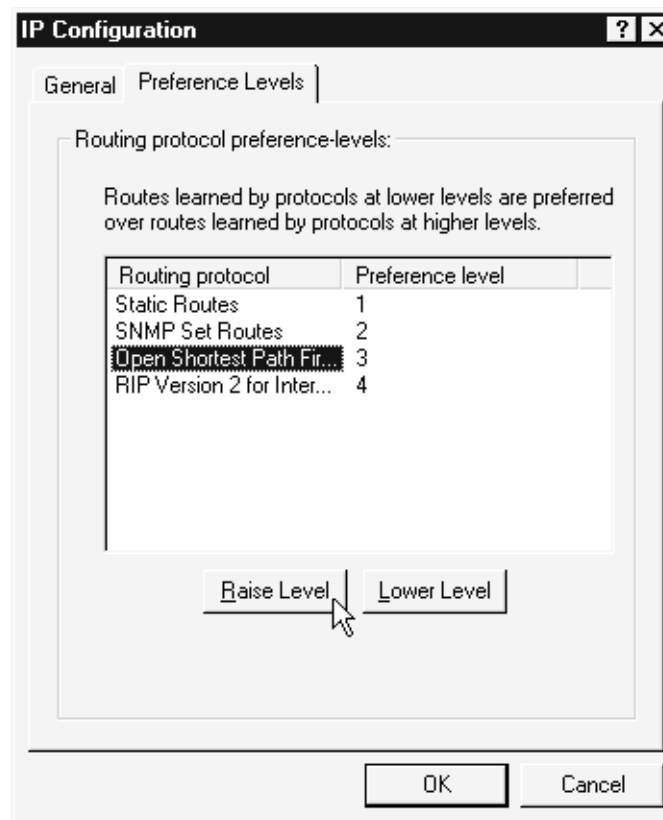
**Highlight
Routing
Protocol**

**Click Level
Button**

Click OK

On the Preference Levels tab page:

1. Highlight a routing protocol
2. Click the Raise Level or the Lower Level button to adjust the protocol's preference level.
3. Click OK.



7.1 Configuring IP Routing

7.1.3 Configuring IP Interfaces

When you configure IP interfaces, you control how the interface will be managed by the switch. Perform this three-part procedure to configure an IP interface:

- Access the IP Configuration Page
- Enable Router Manager and Router Discovery
- Define Packet Filters

In Tree View

**Select
Summary Icon**

**In Display
View**

**Select an
Interface...**

**Right Click to
Display Popup**

**Select
Configure
Interface**

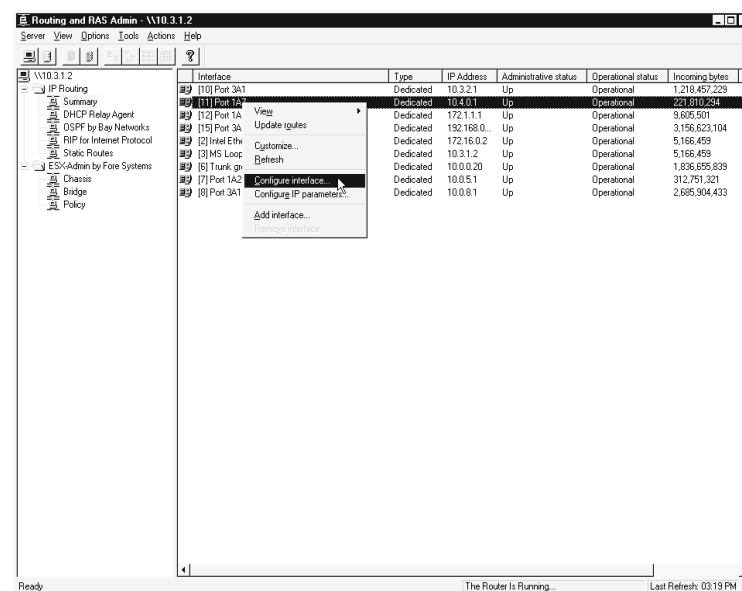
In the Tree View:

1. Select the Summary icon to display a list of the interfaces you can configure.

In the Display View:

2. Select an interface.
3. Right-click to display a popup window.
4. Select the Configure Interface item on the popup window.

Chapter 7 Configuring IP Routing and Protocols



Caution: When defining packet filters, we recommend that you use the FORE Systems Policy facility, accessed from the Tree View, rather than the IP Routing Facility.

The IP Routing facility packet filter screens packets that move between the switch and the NSC on the Adapter 1 interface. It does not filter packets that move between the ports on the switch.

Refer to *Chapter 11–Configuring Policies* in the **ESX Switch Administrator's Guide** for instructions on setting filters for packets that move between ports on the switch.

Enable Router Manager and Router Discovery
To enable the IP router manager and enable router-discovery advertisements:

**On General
Tab Page**

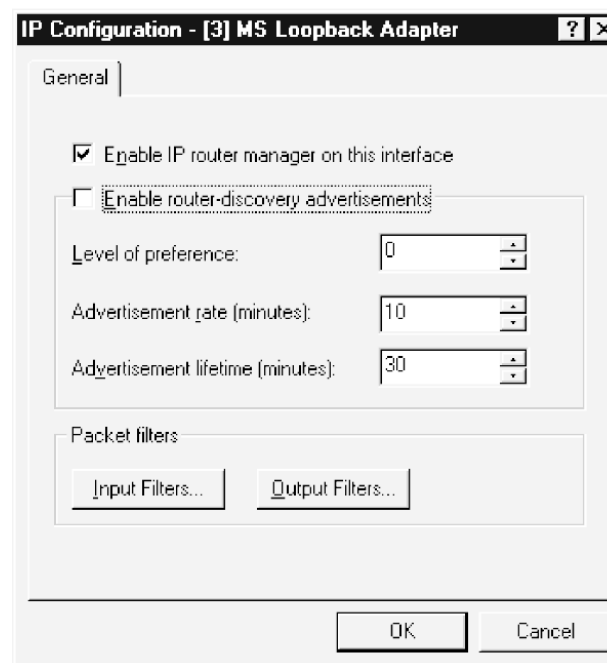
**Enable Router
Manager**

**Enable Router
Discovery**

Click OK

On the General tab page:

1. Select Enable IP router manager for the IP interface to participate in IP routing.
2. Select Enable router-discovery advertisements if the hosts in your network require router discovery to find the first hop router.
3. Click OK.



Note: The default values are shown. for advertisement parameters. Click the ? icon in the menu bar and click on a field to access online help for a particular parameter.

Caution: When you set Packet Filters by clicking the Input Filters and Output Filters buttons and configuring the filters, the switch will filter packets that move between the switch and the NSC on the Adapter 1 interface. The switch will not filter packets that move between the ports on the switch.

Define Packet Filters

To filter IP packets on an interface perform this procedure:

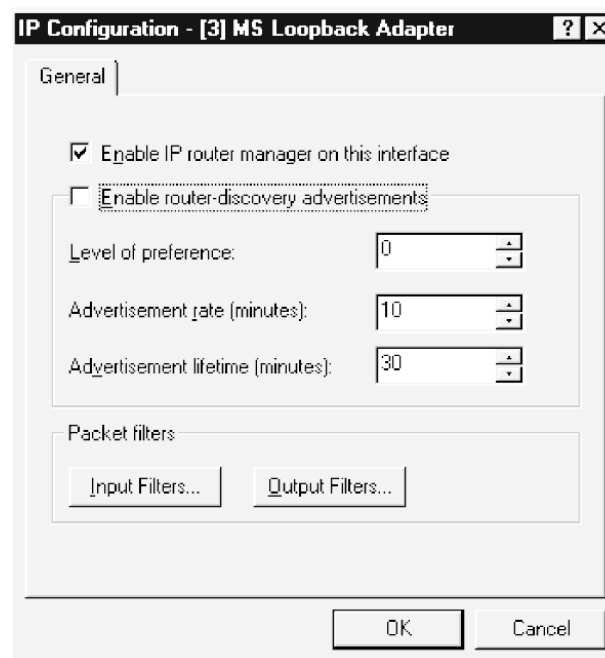
On the General tab page:

1. Click on Input Filters to configure which IP packets are filtered.
2. Click on Output Filters to configure which IP packets are filtered.

When you click on the Input Filters... or Output Filters... button, the IP Packet Filters Configuration page (shown on the following page) will be displayed.

**On General
Tab Page**

**Click on Input
or Output
Filters**



Caution: When setting filters, be aware that the filters you set will only filter packets that are forwarded by NT. Much of the packet traffic routed by the switch bypasses NT. It is routed by the Hardware Forwarding Engine (HFE) from one port to another.

Note: For more information on setting input and output filters, pull down the help menu at the top of the Routing and RAS Admin Screen and read the following topics:

- Adding Local Host Filters
- Setting Input Filters
- Setting output filters

7.1 Configuring IP Routing

Chapter 7 Configuring IP Routing and Protocols

Define Packet Filters (continued)

To set a filter:

**On IP Packet
Filters
Configuration
Page**

**Click the
Add... Button**

**On Add/Edit
IP Filter Page**

**Select Source
and/or
Destination**

**Enter IP
Address and
Mask**

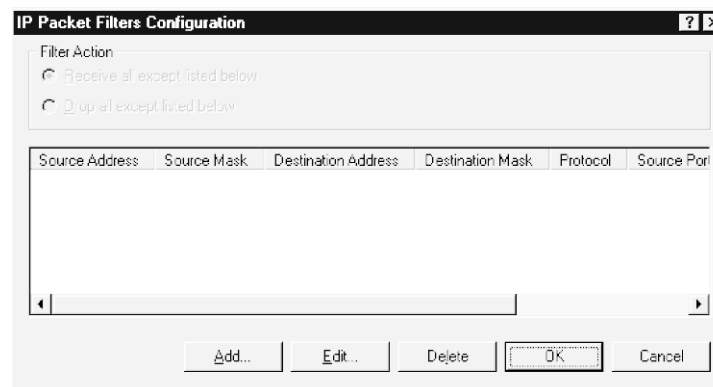
**Select
Protocol**

**Specify
Source or
Destination
Port**

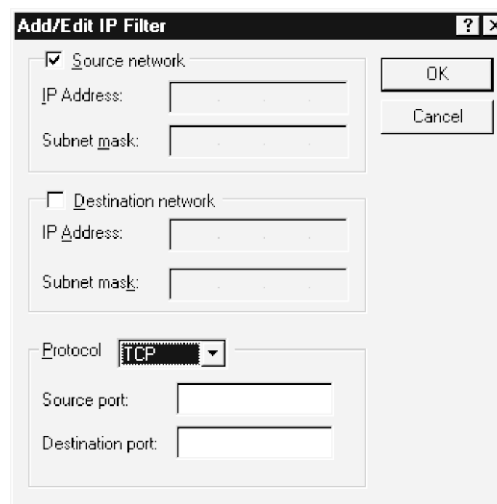
Click OK

On the IP Packet Filters Configuration page:

1. Click the Add... button on the IP Packet Filters Configuration page to set a filter.
The IP Packet Filters Configuration page displays the filters that have been set on the interface.
2. Select Source network and/or Destination network.
3. Enter IP Address and Subnet mask of the IP packets you want to filter.
4. Select protocol.
5. Specify the Source or Destination port if required by the protocol—for example, TCP or UDP.
6. Click OK to add the filter.



The IP Packet Filters Configuration dialog box has a title bar with a question mark and a close button. It contains two radio buttons under 'Filter Action': 'Receive all except listed below' (selected) and 'Drop all except listed below'. Below these is a table with columns: Source Address, Source Mask, Destination Address, Destination Mask, Protocol, and Source Port. The table is currently empty. At the bottom are buttons for 'Add...', 'Edit...', 'Delete', 'OK', and 'Cancel'.



The Add/Edit IP Filter dialog box has a title bar with a question mark and a close button. It has two sections. The first section, 'Source network', is checked and contains fields for 'IP Address' and 'Subnet mask'. The second section, 'Destination network', is unchecked and also contains fields for 'IP Address' and 'Subnet mask'. Below these is a 'Protocol' dropdown menu set to 'TCP', and fields for 'Source port' and 'Destination port'. 'OK' and 'Cancel' buttons are on the right.

7.1 Configuring IP Routing

Chapter 7 Configuring IP Routing and Protocols

7.1.4 Configure a Static ARP Entry

Use the ARP (Address Resolution Protocol) Configuration page to create a permanent binding between a port, a fixed IP address, and a MAC address of a remote host attached to the port. Once established, this binding will not age-out, as will a dynamic ARP-created binding.

In Display
View

Select a Slot

Select Editing
Mode

Select
Configure
Static ARP

Right Click in
Static ARP
Configurations

Select New...

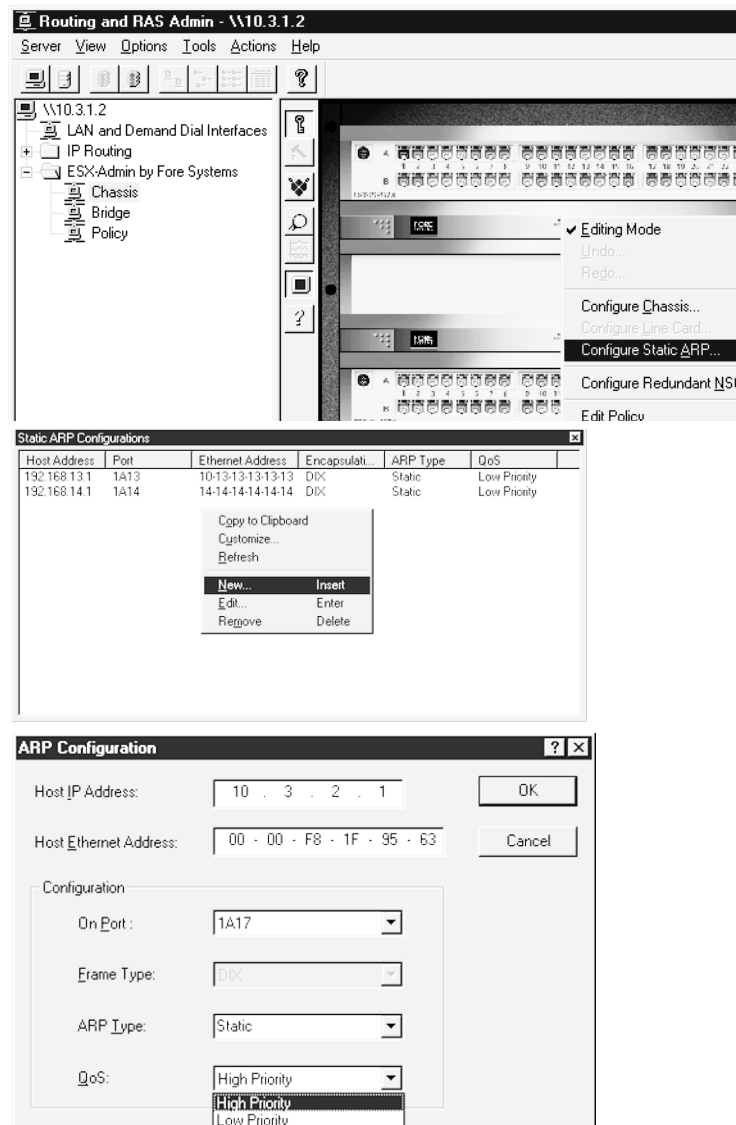
Customize
Port
Configuration

Click OK

In the Display View:

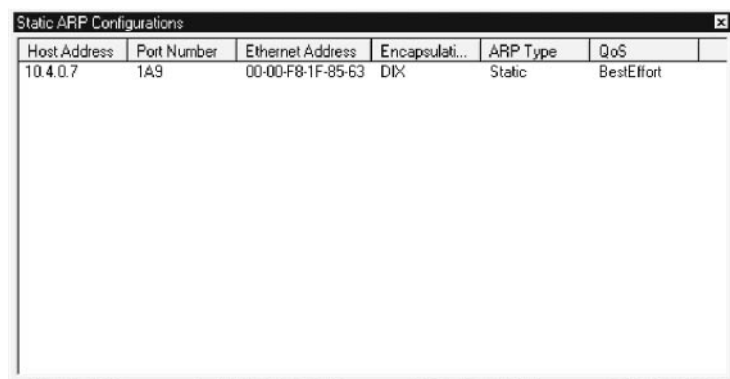
1. Select a slot.
2. Right-click to display the Edit Menu, Select Editing Mode and Right-click again to display the Editing Mode popup with Edit Mode selected.
3. Select the Configure Static ARP item to display the Static ARP Configurations view.
4. Right-click in the Static ARP Configurations view to display a popup.
5. Select the New...Insert item displaying the ARP Configuration page.
6. Configure *Host IP Address* to *Host Ethernet* (MAC) Address to *Port* bindings and set other port parameters—*Arp Type* and Quality of Service (*QoS*)
7. Click OK.

Note:The ARP Table will display the Host Ethernet (MAC) Address.



7.1.4 Configure a Static ARP Entry (continued)

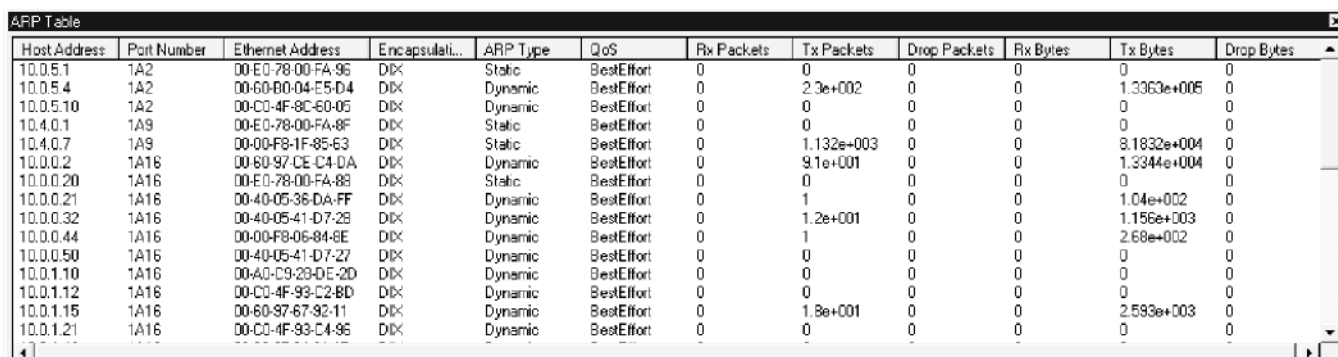
After you configure a Static ARP entry, using the ARP configuration page, the Static ARP Configurations table will show the new configuration.



Host Address	Port Number	Ethernet Address	Encapsulati...	ARP Type	QoS
10.4.0.7	1A9	00-00-F8-1F-85-63	DIX	Static	BestEffort

The ARP table will also show an entry for the configuration you created.

Note: Section 7.1.7, View ARP Table, describes how to display the ARP Table.



Host Address	Port Number	Ethernet Address	Encapsulati...	ARP Type	QoS	Rx Packets	Tx Packets	Drop Packets	Rx Bytes	Tx Bytes	Drop Bytes
10.0.5.1	1A2	00-E0-78-00-FA-96	DIX	Static	BestEffort	0	0	0	0	0	0
10.0.5.4	1A2	00-60-B0-04-E5-D4	DIX	Dynamic	BestEffort	0	2.3e+002	0	0	1.3363e+005	0
10.0.5.10	1A2	00-C0-4F-8C-60-05	DIX	Dynamic	BestEffort	0	0	0	0	0	0
10.4.0.1	1A9	00-E0-78-00-FA-8F	DIX	Static	BestEffort	0	0	0	0	0	0
10.4.0.7	1A9	00-00-F8-1F-85-63	DIX	Static	BestEffort	0	1.132e+003	0	0	8.1832e+004	0
10.0.0.2	1A16	00-60-97-CE-C4-DA	DIX	Dynamic	BestEffort	0	9.1e+001	0	0	1.2344e+004	0
10.0.0.20	1A16	00-E0-78-00-FA-88	DIX	Static	BestEffort	0	0	0	0	0	0
10.0.0.21	1A16	00-40-05-36-DA-FF	DIX	Dynamic	BestEffort	0	1	0	0	1.04e+002	0
10.0.0.32	1A16	00-40-05-41-D7-28	DIX	Dynamic	BestEffort	0	1.2e+001	0	0	1.156e+003	0
10.0.0.44	1A16	00-00-F8-06-84-8E	DIX	Dynamic	BestEffort	0	1	0	0	2.68e+002	0
10.0.0.50	1A16	00-40-05-41-D7-27	DIX	Dynamic	BestEffort	0	0	0	0	0	0
10.0.1.10	1A16	00-A0-C9-29-DE-2D	DIX	Dynamic	BestEffort	0	0	0	0	0	0
10.0.1.12	1A16	00-C0-4F-93-C2-8D	DIX	Dynamic	BestEffort	0	0	0	0	0	0
10.0.1.15	1A16	00-60-97-67-92-11	DIX	Dynamic	BestEffort	0	1.8e+001	0	0	2.593e+003	0
10.0.1.21	1A16	00-C0-4F-93-C4-96	DIX	Dynamic	BestEffort	0	0	0	0	0	0

7.1 Configuring IP Routing

Chapter 7 Configuring IP Routing and Protocols

7.1.5 View TCP/IP Information

Follow the information in this section to display TCP/IP information:

In Tree View

**Select
Summary Icon**

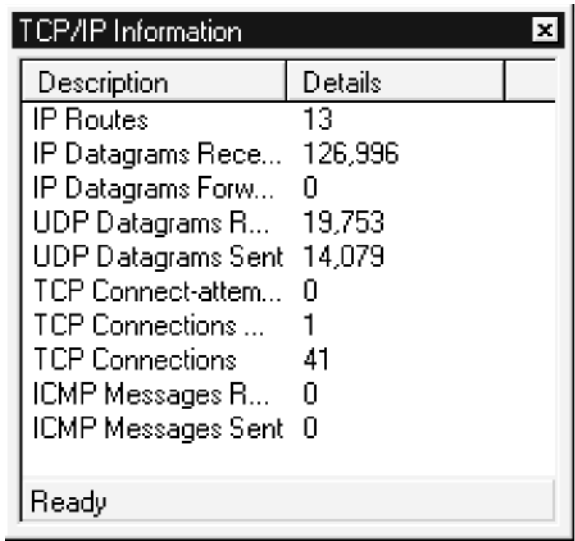
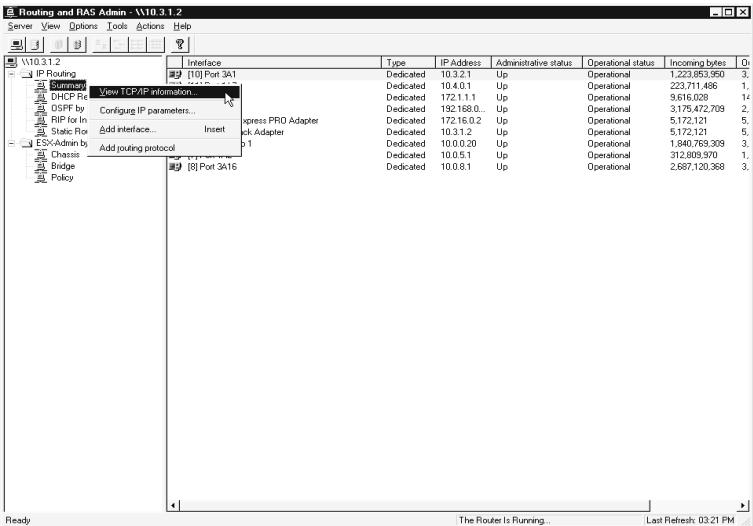
**Right-Click to
Display
Popup**

**Select View
TCP/IP
Information...**

In the Tree View:

1. In Tree View under IP Routing, select the Summary icon.
2. Right-click to display a popup window.
3. Select the View TCP/IP information... item to display the TCP/IP Information screen.

Note: The View TCP/IP Information screen displays information that the switch collects, including: routes, datagrams, connections, and messages



7.1 Configuring IP Routing

Chapter 7 Configuring IP Routing and Protocols

7.1.6 View IP Statistics

Follow the information in this section to display IP Statistics.

Note: This information may be helpful when checking the activity on an interface.

In Tree View

Select Chassis
Icon

Select a Port

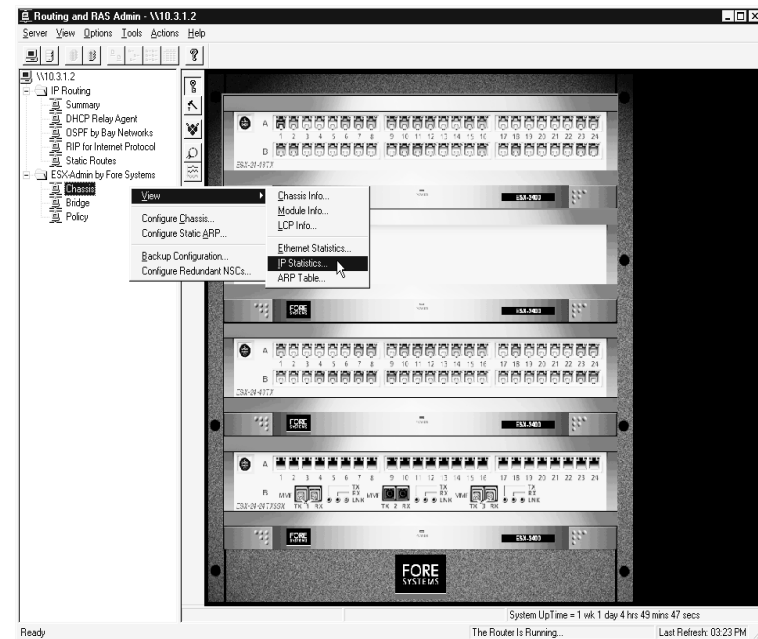
Right-Click to
Display
Popup

Select View
Statistics

Select IP
Statistics

In the Tree View:

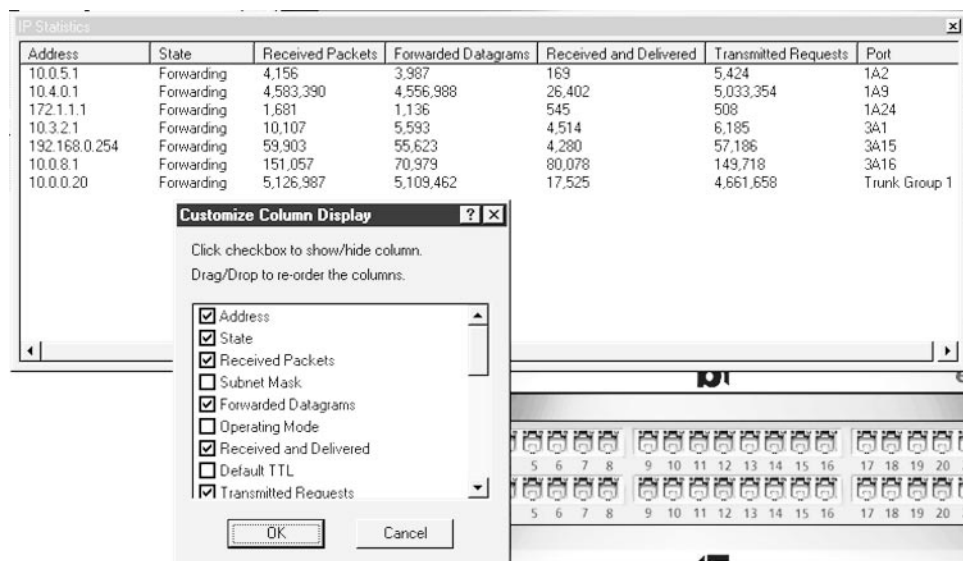
1. In Tree View under ESX-Admin by FORE Systems, select the Chassis icon.
2. Select a port whose statistics you would like to view.
Note: In the example, port 1 is selected.
3. Right-click to display a popup window.
4. Select the View Statistics item and, while holding the mouse button down, move the mouse pointer until IP Statistics is highlighted. Then release the mouse to display IP Statistics (see the following page).



7.1.6 View IP Statistics (continued)

The IP Statistics display shows these parameters for the selected port:

Note: Right click in the IP Statistics table to display the Customize Column Display window. Then click next to the parameter you would like displayed in the IP Statistics table.



Parameter	Description
IP Address	Address of the selected port number.
State	Current state of the port.
Received Packets	Cumulative count.
Forwarded Datagrams	Cumulative count.
Received and Delivered	Cumulative count.
Transmitted Requests	Cumulative count.
Port Number	Port number of the interface whose statistics are displayed in this row.

7.1 Configuring IP Routing

Chapter 7 Configuring IP Routing and Protocols

7.1.7 View ARP Table

Follow the information in this section to display the ARP Table.

Note: This information may be helpful when checking the activity on an interface.

In Tree View

Select Chassis
Icon

Select a Port

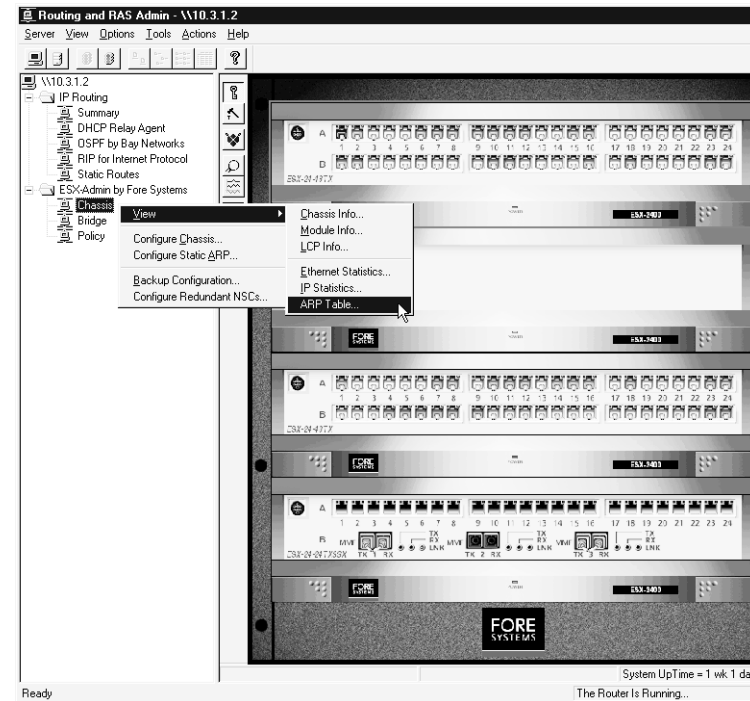
Right-Click to
Display
Popup

Select View

Select ARP
Table

In the Tree View:

1. In Tree View, under ESX-Admin by FORE Systems, select the Chassis icon.
2. Select a port whose statistics you would like to view.
Note: In the example, port 1 is selected.
3. Right-click to display a popup window.
4. Select the View Statistics item and, while holding the mouse button down, move the mouse Table is highlighted. Then release the mouse to display the ARP Table (see the following page).



7.1 Configuring IP Routing

Chapter 7 Configuring IP Routing and Protocols

ARP Table

The ARP Table shows these parameters:

Host Address	Port Number	Ethernet Address	Encapsulati...	ARP Type	QoS	Rx Packets	Tx Packets	Drop Packets	Rx Bytes	Tx Bytes	Drop Bytes
10.0.5.1	1A2	00-E0-78-00-FA-96	DIK	Static	BestEffort	0	0	0	0	0	0
10.0.5.4	1A2	00-60-80-04-E5-D4	DIK	Dynamic	BestEffort	0	2.3e+002	0	0	1.3363e+005	0
10.0.5.10	1A2	00-C0-4F-8C-60-05	DIK	Dynamic	BestEffort	0	0	0	0	0	0
10.4.0.1	1A9	00-E0-78-00-FA-8F	DIK	Static	BestEffort	0	0	0	0	0	0
10.4.0.7	1A9	00-00-F8-1F-85-63	DIK	Static	BestEffort	0	1.132e+003	0	0	8.1832e+004	0
10.0.0.2	1A16	00-60-97-CE-C4-DA	DIK	Dynamic	BestEffort	0	9.1e+001	0	0	1.3344e+004	0
10.0.0.20	1A16	00-E0-78-00-FA-88	DIK	Static	BestEffort	0	0	0	0	0	0
10.0.0.21	1A16	00-40-05-36-DA-FF	DIK	Dynamic	BestEffort	0	1	0	0	1.04e+002	0
10.0.0.32	1A16	00-40-05-41-D7-2B	DIK	Dynamic	BestEffort	0	1.2e+001	0	0	1.156e+003	0
10.0.0.44	1A16	00-00-F8-06-84-8E	DIK	Dynamic	BestEffort	0	1	0	0	2.68e+002	0
10.0.0.50	1A16	00-40-05-41-D7-27	DIK	Dynamic	BestEffort	0	0	0	0	0	0
10.0.1.10	1A16	00-A0-C9-28-DE-2D	DIK	Dynamic	BestEffort	0	0	0	0	0	0
10.0.1.12	1A16	00-C0-4F-93-C2-8D	DIK	Dynamic	BestEffort	0	0	0	0	0	0
10.0.1.15	1A16	00-60-97-67-92-11	DIK	Dynamic	BestEffort	0	1.8e+001	0	0	2.593e+003	0
10.0.1.21	1A16	00-C0-4F-93-C4-96	DIK	Dynamic	BestEffort	0	0	0	0	0	0

Note: Right-click in the Static ARP Configurations display to display a popup, then select the Customize option to view more ARP parameters. You can also configure a new static CRP interface by selecting New... on the popup window.

Parameter	Description
Port number	Port number of the interface.
Host Address	IP address of the host connected to the port.
Logical Port	Number of the port when all ports are numbered sequentially from 1 to N, where N = 384 for an ESX-4800 and 192 for an ESX-2400 switch.
Ethernet Address	MAC address of host connected to the port.
Encapsulation	Frame type of packets sent via this interface.
ARP Type	ARP type enabled on this interface (static, dynamic, etc.).
QoS	Quality of service.

7.2 Configuring OSPF

We recommend that you draw a picture of your network before configuring OSPF. This section uses the example to illustrate how to configure an OSPF network.

Note: Before you can add the OSPF protocol to the switch, you must assign an IP address to the ports used by the switch that will be running OSPF (see Section 7.1). In the example, each router interface requires an IP address.

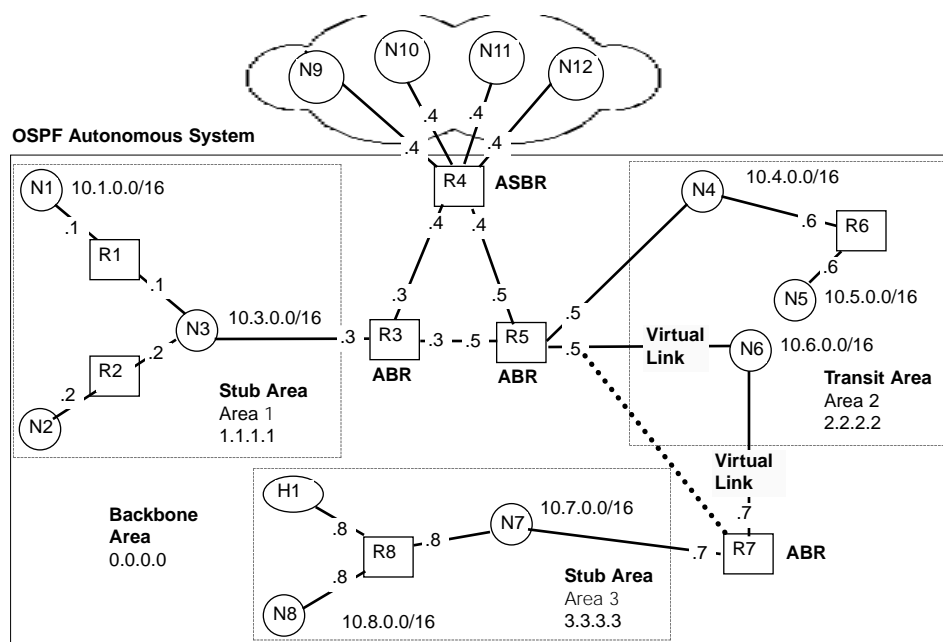


Diagram of a Sample OSPF Configuration

The following sections describe how to configure OSPF:

Task	Section
• Add the OSPF Protocol	7.2.1
• Define the Router's ID and Type	7.2.2
• Assign a Router to an Area	7.2.3
• Set the Router's Interface Parameters	7.2.4
• Set the Border Router's Parameters	7.2.5
• View OSPF Information	7.2.6

Glossary

ABR (Area Border Router) A router that connects more than one area. One of the areas it connects must be the backbone area. It can connect to the backbone, directly, or through a virtual link.

ASBR (Autonomous System Boundary Router) A router that connects the OSPF autonomous system to the outside world.

Backbone area The area that connects the other areas in a network.

Stub area An area that connects to the backbone area directly or connects to the backbone via a virtual link.

Transit area An area directly connected to the backbone area, providing a virtual link to a stub area.

Virtual link An interface that connects a stub area to the backbone through a transit area.

Legend .

Icon	Signifies	Numbers near icon represent
	Area	Area IDs
	Interface	Host portion of Router's interface address
	Network	The network's IP address and mask in CIDR notation.
	Router	The router's ID
	Virtual Link	

7.2.1 Add the OSPF Protocol

The first step in configuring OSPF to run on your network is to add the OSPF protocol to the switch.

In Tree View

**Select IP
Routing Icon
Check Box**

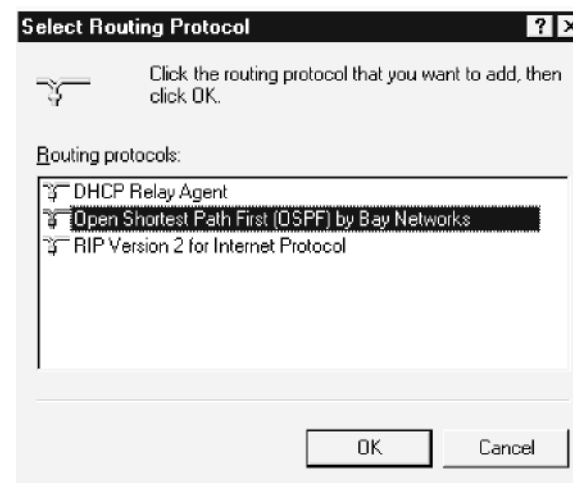
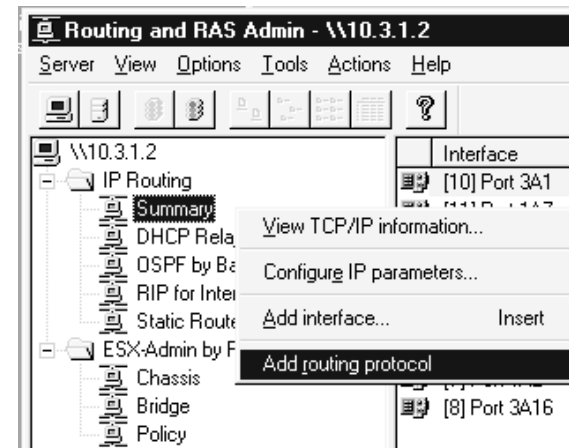
**Right-Click
on Summary
Icon**

**Select Add
Routing
Protocol**

Select OSPF

In the Tree View:

1. Select the check box next to the IP Routing icon to display the Summary icon.
2. Right-click on the Summary icon to display a popup window.
3. Select Add routing protocol menu item to display a dialog box.
4. Select Open Shortest Path First (OSPF) by Bay Networks to display the OSPF Configuration page.



7.2.2 Define the Router's ID and Type

After adding OSPF, you must enter a router ID for each router in your OSPF autonomous system domain. In our example, each of the eight routers has a unique router ID.

Note: To select and define another router, pull down the Server window at the top of the screen, select the Connect to Router item, and enter the router name in the popup window.

On OSPF
Configuration
page

Enter Router
ID

Enable ASBR
Check Box

Select OSPF
Logging
Options

Click OK

On the OSPF Configuration page:

1. Enter the router's ID.

Note: We recommend that you use one of the router's configured IP addresses, although you can use any unique dotted-decimal number.

2. Select the Enable autonomous system boundary router (ASBR) check box if the router will be exchanging routing information with routers outside the OSPF routing domain.

Note: In our example this box would be checked when defining the router ID for router 4.

3. Select OSPF logging options.
4. Click OK to enable selections.

The example shows router identification, and type parameters:

Parameter	Value
Router Identification	Unique identification for a router in an OSPF domain.
Enable autonomous system boundary router	Click the check box and the External Routing tab will appear on the top of the page. Note: Enable only if you plan to inject non-OSPF routes into your domain.
Event logging	Click the ? icon in the menu bar and click on a field to access online help for event logging options.

7.2.3 Assign a Router to an Area

After assigning an ID to a router, assign the router to an area or areas. By assigning area IDs to routers, you create the areas in your network.

On OSPF
Main Page

Select the
Areas Tab

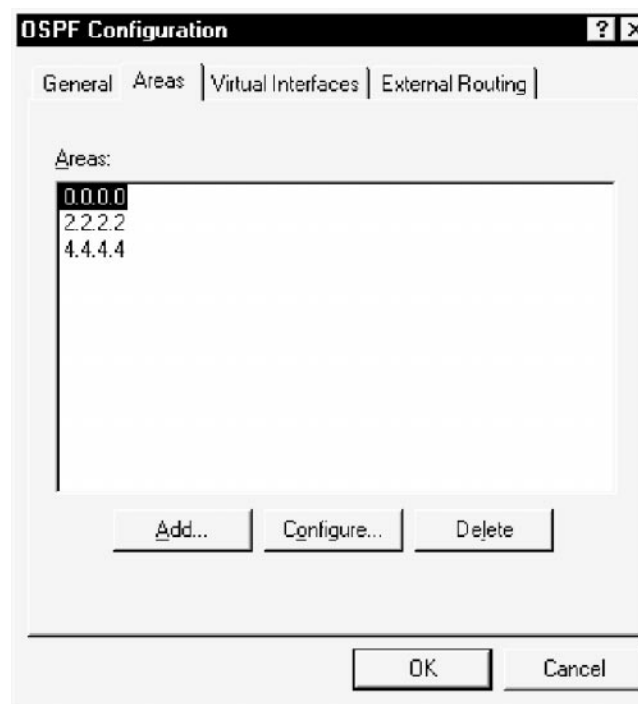
Click the Add
Button

On the OSPF Configuration main page:

1. Select the Areas tab, displaying the Areas tab page.
Note: The Areas: box displays the area IDs defined for the router. After you add an area, it will appear in the box.
2. Click the Add button to display the OSPF Area Configuration General tab page (see the following page).

Our example contains four areas. Each area has an area ID and belongs to one of the following area types.

<u>Area ID :</u>	<u>Area Type</u>
0.0.0.0	Backbone area
1.1.1.1	Stub area
2.2.2.2	Transit area
3.3.3.3	Stub area



The table shows the area membership of each router in the OSPF example:

<u>Area ID :</u>	<u>R1</u>	<u>R2</u>	<u>R3</u>	<u>R4</u>	<u>R5</u>	<u>R6</u>	<u>R7</u>	<u>R8</u>
0.0.0.0			✓	✓	✓			
1.1.1.1	✓	✓	✓					
2.2.2.2					✓	✓	✓	
3.3.3.3							✓	✓

7.2.3 Assign a Router to an Area or Areas (continued)

Continue the procedure started on the previous page to assign the routers to areas.

On OSPF Area Configuration Page

Enter the Area ID

Check Enable Clear-Text Passwords

Check Stub Area Check Box (optional)

Click OK

On the OSPF Area Configuration page:

1. Enter the Area ID in the Area ID box—a 32 bit, dotted decimal number.
 2. Check Enable clear-text passwords if appropriate.
 3. Check the Stub area check box if appropriate.
 4. Click OK to return to the OSPF Configuration page.
- Note:** that the Area ID(s) you added will appear in the Area Box.

Enable clear text password – The default setting (selected) allows passwords to be used on the area.

Note: If this box remains selected, all interfaces in the same area must use identical passwords. To configure passwords on an interface. See Section 7.2.4, "Set the Router's Interface Parameters."

Select the Stub area check box if:

- You do not want to have external routes flooded into the area.

Or

- If the area is not a backbone area and does not provide a virtual link for another stub area

Note: After selecting the Stub area check box, you can configure the Stub metric and Import summary advertisements check boxes. Click the ? icon in the menu bar and click on a field to access online help.

7.2.4 Set the Router's Interface Parameters

After configuring the areas on your network, configure the router interfaces that you want to run OSPF, and perform the following tasks:

- Define the Interface 's Attributes
- Define the Interface's Neighbors
- Set the Interface's Timing and MTU Size Parameters

Define the Interface's Attributes

In this two-part procedure, first select the interface you want to configure. Then define the interface's attributes.

To select the interface:

In Tree View

**Right-Click
OSPF by Bay
Networks Icon**

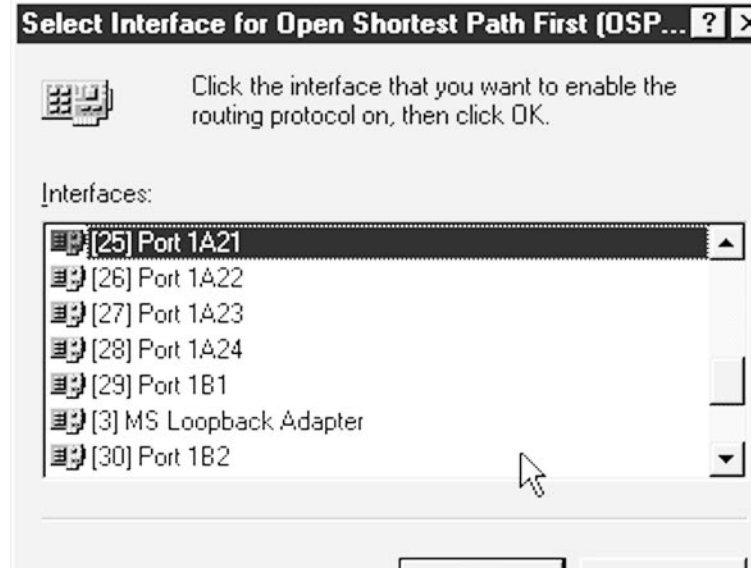
**Select Add
Interface**

**Double Click
an Interface**

In the Tree View:

1. Right-click OSPF by Bay Networks icon to display popup window.
2. Select Add Interface to display the Select Interface for OSPF window.
3. Double click the interface you want to configure to display the OSPF Configuration page showing the Port number of the interface on the top of the page.

Note: Continue defining the interfaces attributes as described on the next page.



Note: If you want to manage the switch over the OSPF network, you will need to:

- Assign an IP address to adapter 3 "**[3] MS Loopback Adapter**"—see Section 4.2, "Startup Sequence" for details.
- Configure adapter 3's interface, the internal IP address of the switch, to run the OSPF protocol as described in this section.

Define the Interface's Attributes (continued)

After selecting the interface you want to configure, define the interface's attributes.

On the OSPF Configuration page

Modify General Tab Page

Click OK

On the OSPF Configuration page:

1. Modify the OSPF Configuration General tab page to define the interface attributes.
2. Click OK

The example shows OSPF configuration parameters

Parameter	Value
Enable OSPF	Select to enable OSPF on this interface.
Area ID	OSPF area where the Interface resides.
Priority	Priority for being elected designated router (A zero value means the router is not eligible to be elected).
Cost	The value OSPF will advertise as the cost for using the interface.

OSPF Configuration - [18] Port 1A15

General | Neighbors | Advanced

☒ Enable OSPF on this interface

Area ID: 0.0.0.0

Router priority: 1

Cost: 2

Password:

Type:

☒ Broadcast

☐ Point-to-point

☐ NBMA

OK Cancel

Parameter	Value
Password	If using passwords you must first enable them, see <i>Section 7.2.3, "Assign a Router to an Area or Areas"</i> .
Type	We recommend that you use broadcast Note: If you select NBMA (Non-broadcast, multi-access) you must define the interface's neighbors, as described in the following section.

Define the Interface's Neighbors

In this two-part procedure, first, select the interface you want to configure. Then define the interface's neighbors.

To select the interface:

In Tree View

**Right-Click
OSPF by Bay
Networks Icon**

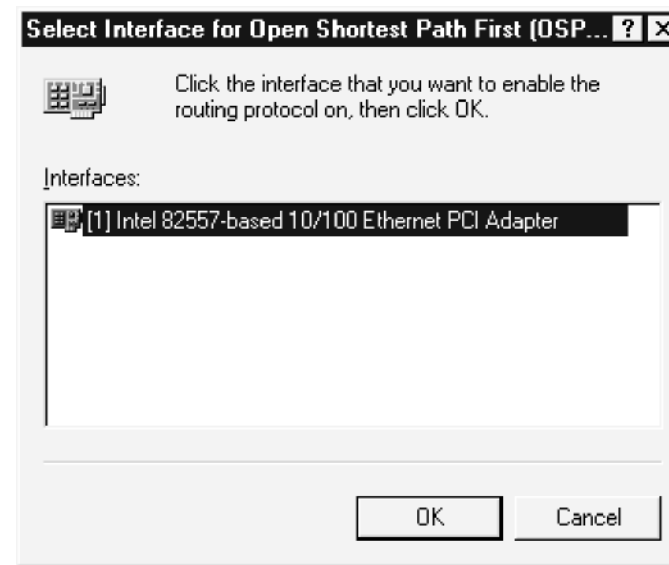
**Select Add
Interface**

**Double Click
an Interface**

In the Tree View:

1. Right-click the OSPF by Bay Networks icon to display a popup window.
2. Select Add Interface to display the Select Interface for OSPF window.
3. Double click the interface you want to configure to display the OSPF Configuration page showing the Port number of the interface on the top of the page.

Note: Continue this procedure on the next page.



7.2 Configuring OSPF

Chapter 7 Configuring IP Routing and Protocols

Define the Interface's Neighbors (continued)

After selecting the interface you want to configure, define the interface's neighbors:

Note: We recommend that you use broadcast rather than NBMA.

On the OSPF
Configuration
page

Enter the
Neighbor's
Address and
Priority

Click Add

Click OK

On the OSPF Configuration page:

1. Enter the Neighbor's address and priority.
2. Click Add and the values you entered for Address and priority will appear in the NBMA neighbors: box.
3. Click OK.

OSPF Configuration - [2] DEC DE500 Fast Ethernet... ? X

General Neighbors Advanced

NBMA neighbors:

Address	Priority
10.3.2.2	1

Add Remove

Neighbor:

Address: Priority: 1

OK Cancel

Note: Use NBMA (Non-broadcast multi-access) if you want the interface to behave as a non-broadcast, multi-access media. See online help for details.

To use NBMA you must select the NBMA radio button, described in the previous section, "Define the Interface's Attributes".

Set the Interface's Timing and MTU Size Parameters

In this two-part procedure, First, select the interface you want to configure. Then define the interface's parameters.

To select the interface:

In the Tree View:

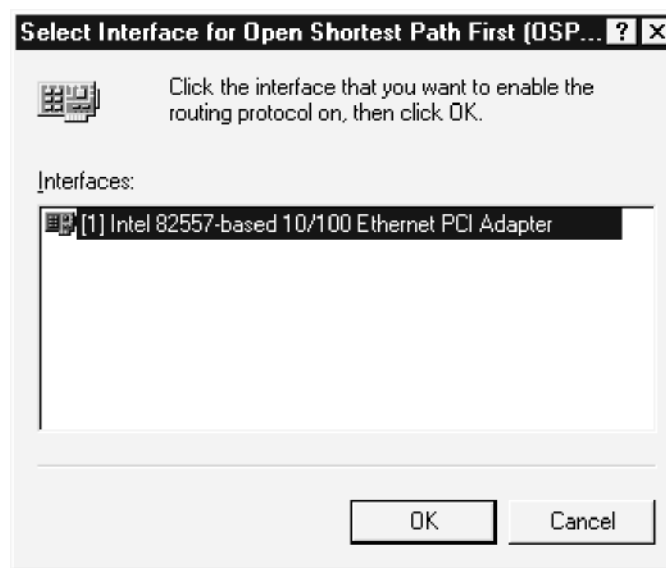
In Tree View

**Right-Click
OSPF by Bay
Networks Icon**

**Select Add
Interface**

**Double Click
an Interface**

1. Right-click OSPF by Bay Networks icon to display popup window.
2. Select Add Interface to display the Select Interface for OSPF window.
3. Double click the interface you want to configure. The OSPF Configuration page displaying the Port number of the interface on the top of the page will appear
Note: Continue defining the interface's attributes as described on the next page.



Set the Interface's Timing and MTU Size Parameters (continued)

After selecting the interface you want to configure, define the interface's Timing and MTU size parameters:

On the OSPF Configuration page

Select the Advanced Tab

Modify Default Timing and MTU Size Values

Click OK on Advanced Tab Page

Click OK on General Tab Page

On the OSPF Configuration page:

1. Select the Advanced tab.
2. Modify the default values on the OSPF Configuration Advanced tab page.
3. Click OK on the Advanced tab page to change the default configuration.
4. Click OK on the General tab page to have the change take effect.

The example shows the default parameters for the interface.

The screenshot shows the 'OSPF Configuration - [18] Port 1A15' dialog box. The 'Advanced' tab is selected, showing the following parameters and their default values:

Parameter	Value
Transit delay (seconds):	1
Re-transmit interval (seconds):	5
Hello interval (seconds):	10
Dead interval (seconds):	40
Poll interval (seconds):	120
MTU size (bytes):	1500

At the bottom of the dialog are 'OK' and 'Cancel' buttons. A help icon (?) is visible in the top right corner of the dialog's title bar.

Click the ? icon in the menu bar and click on a field to access online help.

7.2.5 Configure the Router's Border Parameters

After setting the router's interface parameters, you may need to configure its border parameters, as described in the following subsections:

- Assign Virtual Links to Area Border Routers
- Provide Summary Advertisements to the Backbone
- Control External Routing Information Distributed inside the OSPF Domain
- Set External Route Filters

Assign Virtual Links to Area Border Routers

When configuring a virtual link, each router on either side of the virtual link must add and configure a virtual interface. To assign virtual links to an area border router, follow this two-part procedure:

- Access the OSPF Virtual Interface Configuration page
- Assign and configure the virtual link

To access the OSPF Virtual Interface Configuration page:

**On the OSPF
Configuration
page**

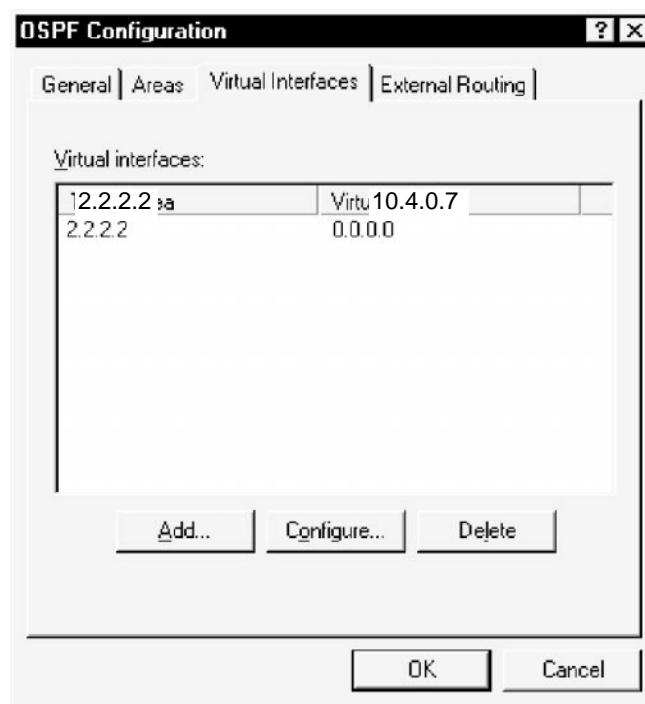
**Select Virtual
Interfaces Tab
Page**

Click Add

**On the Virtual Interfaces tab
page:**

1. Select the Virtual Interfaces tab page.
2. Click Add to display the Virtual Interfaces tab page.

<u>Parameter</u>	<u>Value indicates:</u>
Transit area	The area providing transit access to the backbone.
Virtual neighbor	The router ID of the virtual neighbor.



Note: For each router on either side of the virtual link, you need to add and configure a virtual interface.

- In the Sample OSPF Diagram shown in *Section 7.2, "Configuring OSPF"*, ABR's R5 and R7 provide a virtual link through area 2—a *transit area*—and connect area 3—a *stub area*—to the backbone
- Both router 5 and router 7 need to define each other as virtual neighbors, and list area 2 as the transit area.
- The Virtual interfaces window shown above provides the configuration from R7's point of view.

**Assign Virtual Links to an Area Border Router
(continued)**

To configure the virtual link:

**On Virtual
Interface
Configuration
Page**

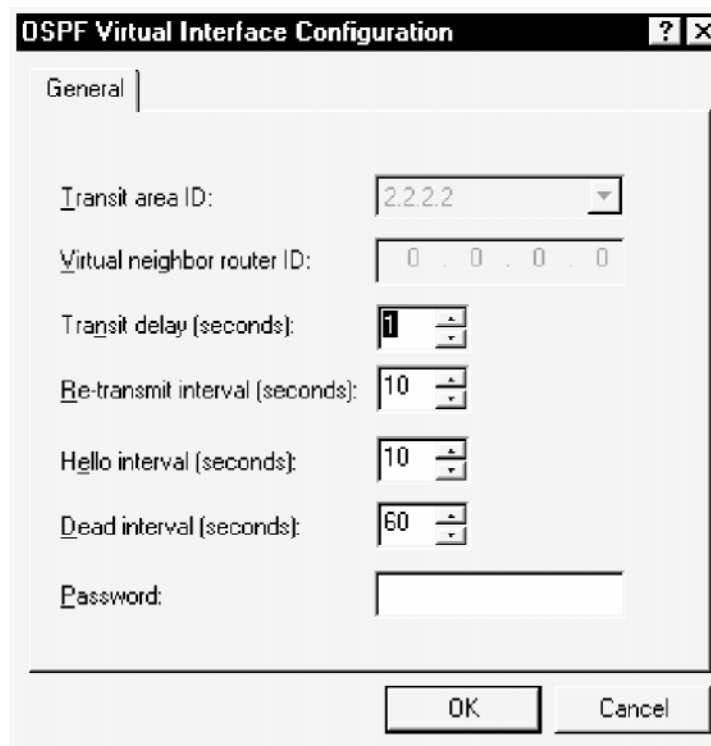
**Set the Timing
Parameters**

**Set the
Password**

Click OK

**On the Virtual Interface
Configuration page:**

1. Set the timing parameters.
2. Set the password for the interface, if passwords are enabled.



The image shows a screenshot of the 'OSPF Virtual Interface Configuration' dialog box. The 'General' tab is selected. The fields and their values are: Transit area ID: 2.2.2.2; Virtual neighbor router ID: 0.0.0.0; Transit delay (seconds): 1; Re-transmit interval (seconds): 10; Hello interval (seconds): 10; Dead interval (seconds): 60; Password: (empty). The 'OK' and 'Cancel' buttons are at the bottom right.

Field	Value
Transit area ID:	2.2.2.2
Virtual neighbor router ID:	0 . 0 . 0 . 0
Transit delay (seconds):	1
Re-transmit interval (seconds):	10
Hello interval (seconds):	10
Dead interval (seconds):	60
Password:	

3. Click OK.

The parameter values shown in the example are the default values. Click the ? icon in the menu bar and click on a field to access online help.

Provide Summary Advertisements to the Backbone

When aggregating advertisements within an area into the backbone, this procedure describes how to define the range of addresses to aggregate.

Specifying ranges for an area minimizes the advertisements that an Area border Router advertises, allowing Routers outside the area are able to reduce the size of their routing tables.

This two-part procedure describes how to provide summary advertisements to the backbone:

- Select the area
- Define the range

To select the area:

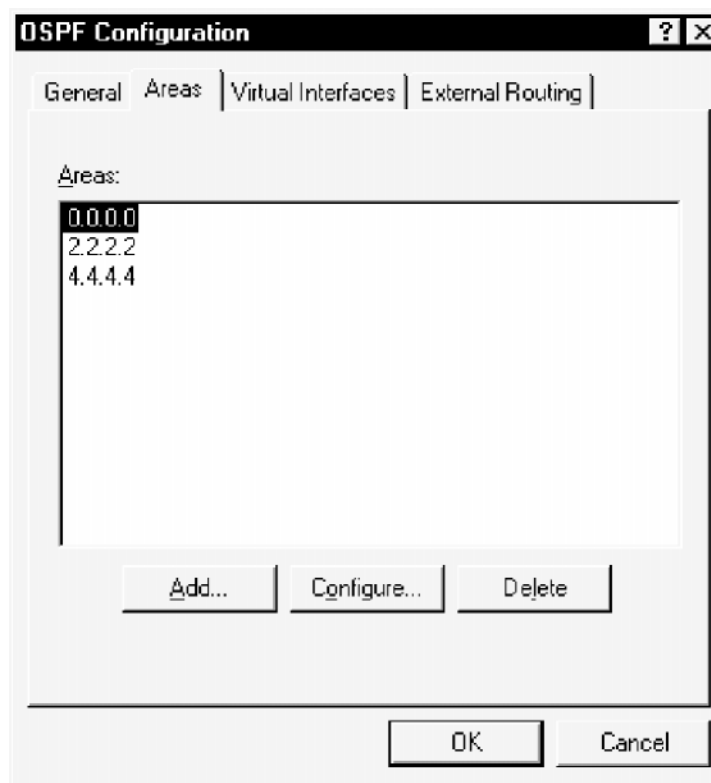
On Areas Tab Page

Highlight the Area ID

Click Configure

On the Areas tab page:

1. Highlight the Area ID of the area whose routes you want to aggregate into the backbone.
2. Click Configure to display the OSPF Area Configuration page.



In the OSPF example, three areas provide advertisements to the backbone:

<u>Area ID</u>	<u>Area Type</u>
1.1.1.1	Stub area
2.2.2.2	Transit area
3.3.3.3	Stub area

Provide Summary Advertisements to the Backbone (continued)

To define the range of addresses to aggregate for the area you selected on the previous page:

On OSPF Area
Configuration
Page

Select the
Ranges Tab

Enter Range
Address and
Mask

Click OK

On the OSPF Area Configuration page:

1. Select the Ranges tab to display the Ranges tab page.
2. Enter the Range Address and Mask that summarize the area's routes.
3. Click OK.

The screenshot shows the 'OSPF Area Configuration' dialog box with the 'Ranges' tab selected. The 'Ranges' section contains a table with two columns: 'Address' and 'Mask'. The first row shows '11.1.0.0' and '255.255.0.0'. Below the table are 'Add' and 'Remove' buttons. At the bottom, there are input fields for 'Range:', 'Address:', and 'Mask:', followed by 'OK' and 'Cancel' buttons.

Address	Mask
11.1.0.0	255.255.0.0

Buttons: Add, Remove

Range: Address: Mask: OK Cancel

Note: Each address range consists of an address and a subnet mask that describe the collection of IP addresses within the networks attached to the area border router.

Control External Routing Protocols Distributed inside the OSPF Domain

Perform this procedure if your OSPF network contains Autonomous System Boundary Routers (ASBR's). See *Section 7.2.2, Define the Router's ID and Type*. ASBR's are connected to areas outside the OSPF domain. They control the routing information that routers in the OSPF domain can receive.

This procedure describes how to establish protocol-based filters that control External (non-OSPF) routing protocols that are distributed within the OSPF domain by the ASBR's in your OSPF network. The procedure has two parts:

- Enable the switch as an ASBR
- Define external protocol filters

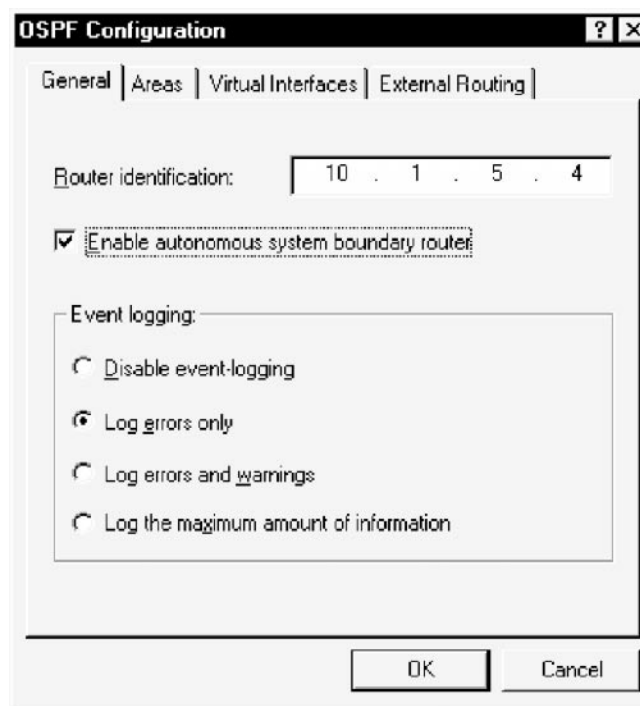
To enable an ASBR:

**On OSPF
Configuration
General Tab
Page**

**Check ASBR
Check Box**

On the OSPF Configuration General tab page:

1. Check the Enable autonomous system boundary router check box to display the External Routing tab page (shown on the next page).



In the Sample OSPF Diagram shown in *Section 7.2, "Configuring OSPF"*, router 4 is an ASBR.

Note: Information on setting address-based route filters to control the external routes that routers in the OSPF domain can receive is presented in the next section, *"Control External Routes Distributed inside the OSPF Domain"*.

Select the Log the maximum amount of information setting when trying to troubleshoot a problem.

Control External Routing Protocols Distributed inside the OSPF Domain (continued)

Continue this procedure to define the external protocols that will be distributed inside the OSPF domain.

Note: External OSPF routes are redistributed into the OSPF domain.

On External Routing Tab Page

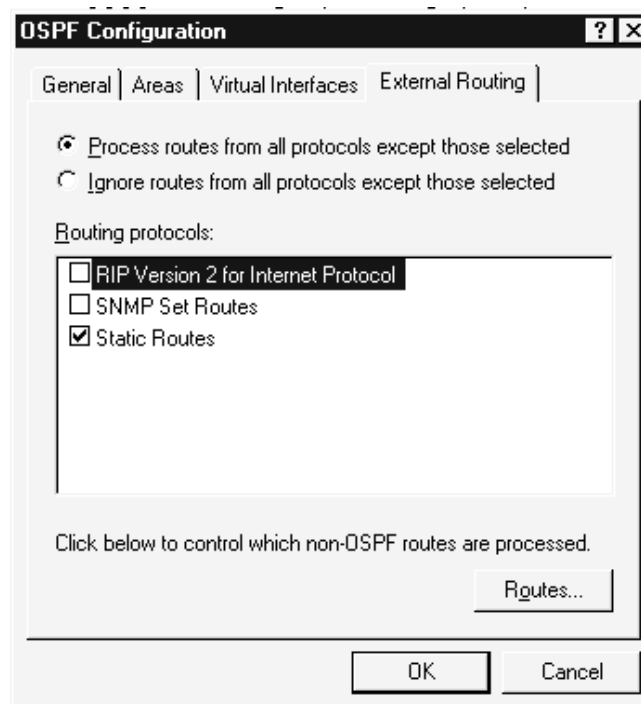
**Select:
“Process...” or
“Ignore...”**

Select Routing Protocols

Click OK

On the External Routing tab page:

1. Select the Routing protocols.
2. By clicking a radio button, choose to either:
 - process all the protocols except those you select in the next step
 - OR
 - ignore all the protocols except those you select in the next step.
3. Select the protocols.
4. Click OK.



The example shows that only Static Routes are being redistributed into OSPF—all other routes are being ignored.

Control External Routes Distributed inside the OSPF Domain

Perform this procedure if your OSPF network contains Autonomous System Boundary Routers (ASBR's). See *Section 7.2.2, "Define the Router's ID and Type"*. ASBR's are connected to areas outside the OSPF domain. They control the routing information that routers in the OSPF domain can receive.

This procedure describes how to establish route-based filters that control External (non-OSPF) routes that are distributed inside the OSPF domain by the ASBR's in your OSPF network. The procedure has three parts:

- Enable the switch as an ASBR
- Access the OSPF External Routes page
- Define External route filters

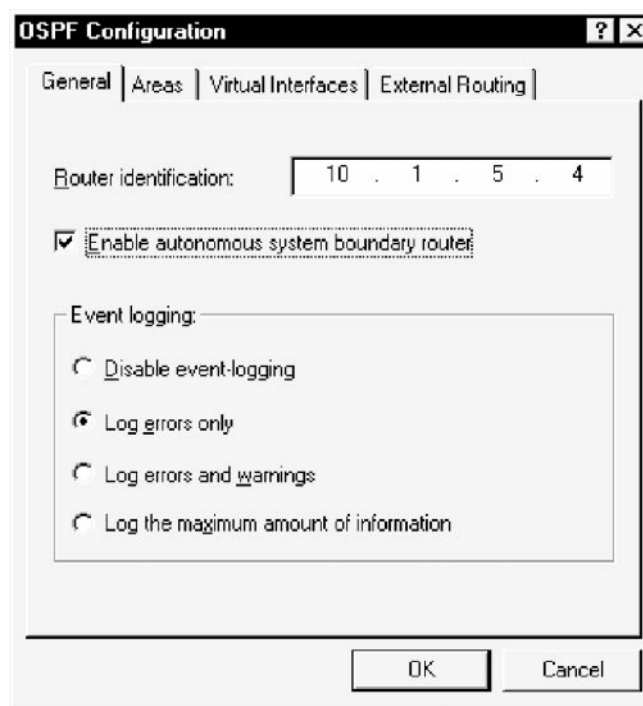
To enable an ASBR:

**On OSPF
Configuration
General Tab
Page**

**Check ASBR
Check Box**

On the OSPF Configuration General tab page:

1. Check the Enable autonomous system boundary router check box to display the External Routing tab page (shown on the next page).



In the Sample OSPF Diagram shown in *Section 7.2, "Configuring OSPF"*, router 4 is an ASBR.

Note: Information on setting protocol-based route filters to control the external routes that routers in the OSPF domain can receive is presented in the previous section, "*Control External Routing Protocols Distributed inside the OSPF Domain*".

Control External Routes Distributed inside the OSPF Domain (continued)

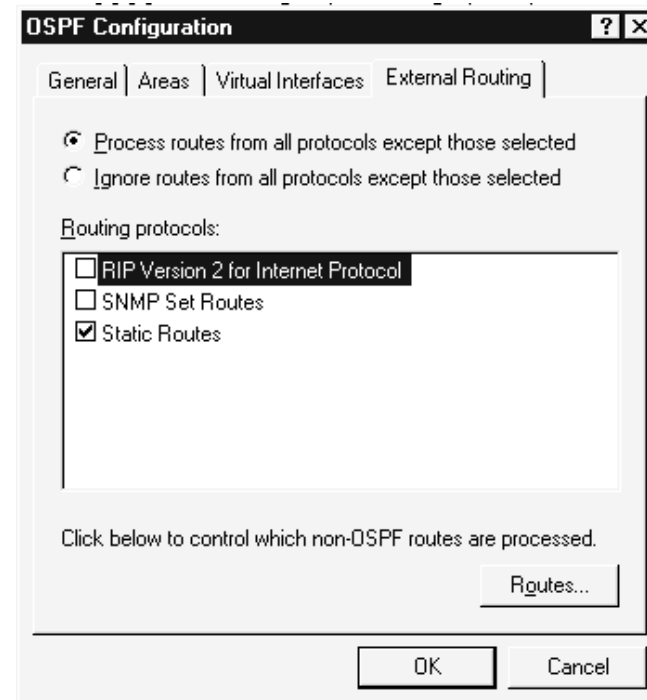
Continue this procedure to access the OSPF External Route Filters page.

**On External
Routing Tab
Page**

**Select the
Routes Button**

On the External Routing tab page:

1. Select the Routes button to access the OSPF External Route Filters page shown on the following page.



Control External Routes Distributed inside the OSPF Domain (continued)

The External Route Filters page allows you to control the external routes being distributed within the OSPF domain.

**On External
Route Filters
Page**

**Select:
“Process...” or
“Discard...”**

**Enter Route
Address and
Mask**

Click Add

Click OK

On the External Route Filters page:

1. Click on the Routes... button to display the OSPF External Route Filters page.

2. By clicking a radio button, choose to either:

- process all the routes except those you list in the next step

OR

- discard all the routes except those you select in the next step.

3. Enter the route address and mask.

4. Click Add.

Note: The information you add will appear in the Routes: box.

5. Click OK to have the information in the Routes: box take effect.

OSPF External Route Filters ? x

☒ Process all routes except those listed
☐ Discard all routes except those listed

Routes:

Address	Mask
11.1.0.0	255.255.0.0

Add Remove

Route

Address: Mask:

OK Cancel

Click the ? icon in the menu bar and click on a field to access online help.

7.2.6 View OSPF Information

Follow the information in this section to display the following OSPF information:

- OSPF Areas
- Link State Database
- Neighbors
- Virtual Interfaces

In Tree View

Select OSPF
Icon

In Tree View

Right-Click to
Display
Popup

Click View
and Hold to
Display Items

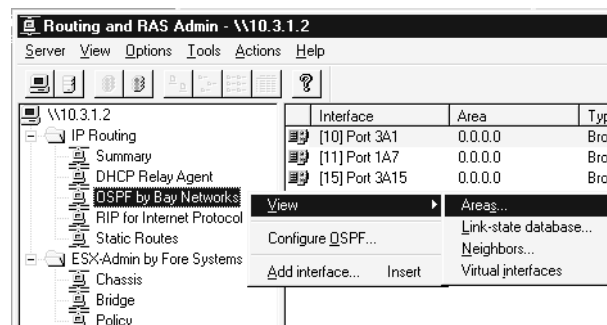
Select Item to
View

In the Tree View:

1. In Tree View, select OSPF by Bay Networks icon.
2. In the Tree view, right click to display popup window.
3. Click the view selection and hold to display a second popup listing view items.
4. While holding, move the mouse to the item you want to view and release the mouse button.

Note: OSPF view selections are described in the following sections:

- OSPF Areas
- Link State Database
- Neighbors
- Virtual Interfaces



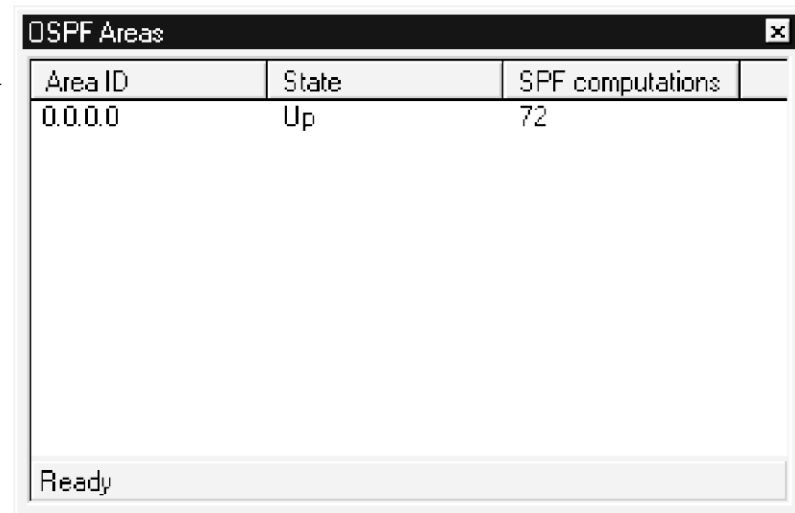
OSPF Areas

The OSPF Areas display shows parameter values for the four areas that were configured in creating the OSPF example.

<u>Area ID</u>	<u>Area Type</u>
0.0.0.0	Border area
1.1.1.1	Stub area
2.2.2.2	Transit area
3.3.3.3	Stub area

OSPF Areas displays the following parameters:

<u>Parameter</u>	<u>Description</u>
Area IDs	The ID of each area configured in the OSPF domain.
State	The operational state of the area: Up or Down.
SPF Computations	The cumulative number of Shortest Path First (SPF) computations performed by the router on this area since the router started.



OSPF Areas		
Area ID	State	SPF computations
0.0.0.0	Up	72

Ready

Link State Database

The Link State Database display shows the link state information calculated for configured areas.

OSPF Link State Database			
Area ID	Type	Link state ID	Advertising router
0.0.0.0	Router	10.140.1.20	10.140.1.20
0.0.0.0	AS External	0.0.0.0	10.140.1.20
0.0.0.0	AS External	10.0.0.0	10.140.1.20
0.0.0.0	AS External	10.0.1.48	10.140.1.20
0.0.0.0	AS External	10.140.1.20	10.140.1.20
0.0.0.0	Stub	10.140.1.0	10.140.1.20

Link State Database displays the following parameters per Link State entry:

<u>Parameter</u>	<u>Description</u>
Area ID	The area ID of the area whose link state information is being displayed.
Type	The Link State advertisement type.
Link state ID	Often the router ID of the advertising router.
Advertising router	The router ID of the router that originated this Link State advertisement.
Age	The age of the advertisement.
Sequence	Used by OSPF to determine the newest advertisement.

OSPF Neighbors

The OSPF Neighbors display shows the following parameters:

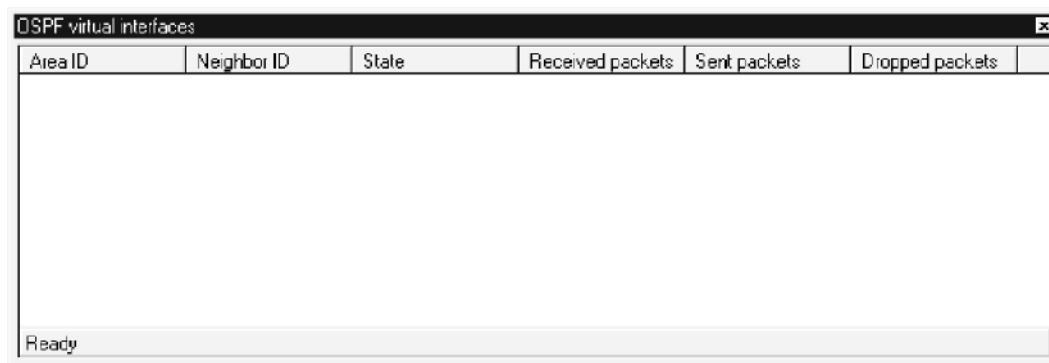
OSPF Neighbors				
Neighbor	Neighbor ID	Type	State	Priority
10.0.0.21	10.0.0.21	Dynamic	Full	1
◀				
Ready				

Parameter	Description
Neighbor	The neighbor's IP address.
Neighbor ID	The neighbor's router ID.
Type	<i>Dynamic</i> if router discovery is enabled, or <i>static</i> if routes are configured.
State	State of the OSPF adjacency with this neighbor. <i>Full</i> if completely established.
Priority	Router's priority to become the designated router.

Note: The table shows all neighbors including virtual-configured routers.

Virtual Interfaces

OSPF Virtual Interfaces displays the following parameters:



Area ID	Neighbor ID	State	Received packets	Sent packets	Dropped packets
---------	-------------	-------	------------------	--------------	-----------------

Ready

<u>Parameter</u>	<u>Description</u>
Area ID	The transit area's ID.
Neighbor ID	The router ID of the virtual-neighbor router that connects to the other side of the transit area.
State	State of the OSPF adjacency with this neighbor. <i>Full</i> if completely established.

7.3 Configuring RIP

We recommend that you draw a picture of your network, before configuring RIP. The following diagram provides an example. This section uses this sample RIP configuration to illustrate how to configure a RIP network.

Before configuring RIP, assign IP addresses to the ports used by the routers that will be running RIP (see Section 7.1). The following sections describe how to configure RIP:

Task	Section
• Add the RIP Protocol	7.3.1
• Configure the RIP Protocol	7.3.2
• Set the Router's Interface Parameters	7.3.3
• View RIP Information	7.3.4

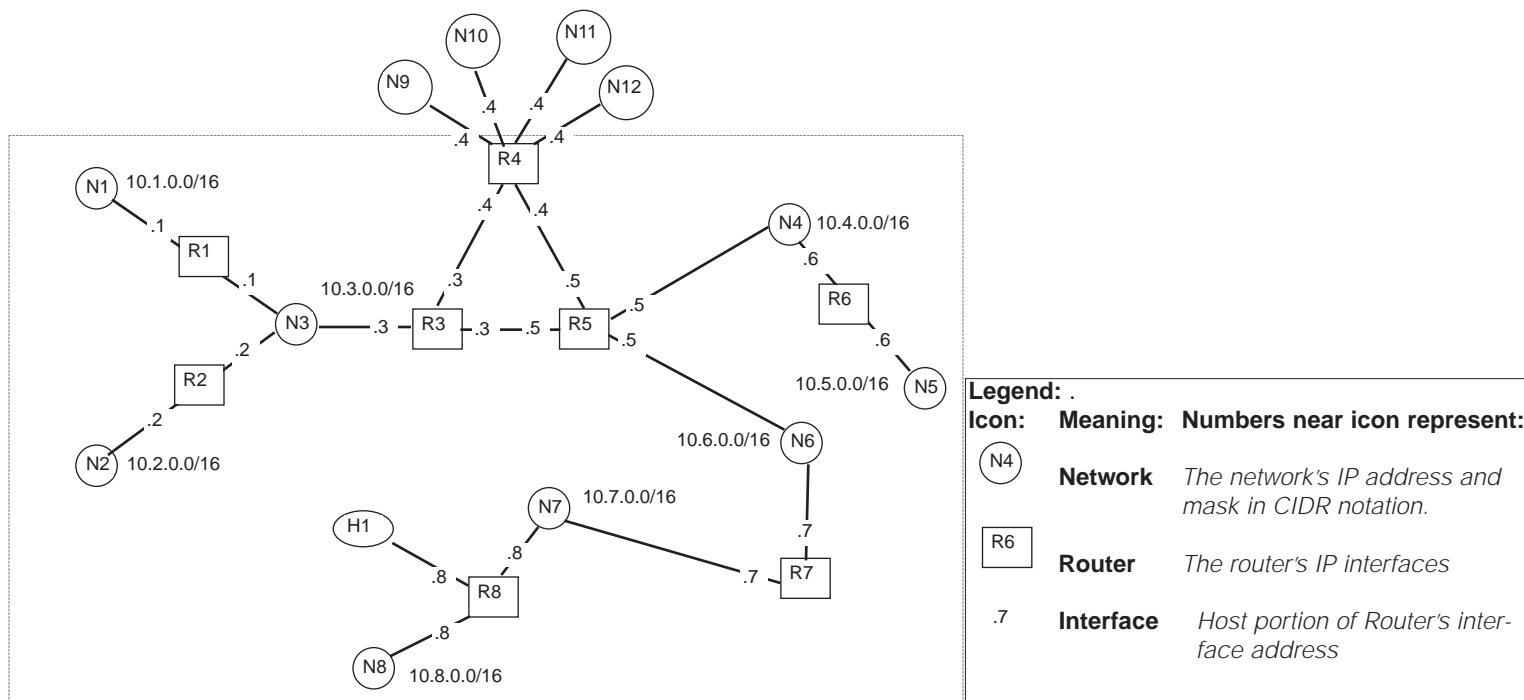


Diagram of a sample RIP configuration

7.3.1 Add the Rip Protocol

The first step in configuring RIP to run on your network is to add the RIP protocol.

In Tree View

**Select IP
Routing Icon
Check Box**

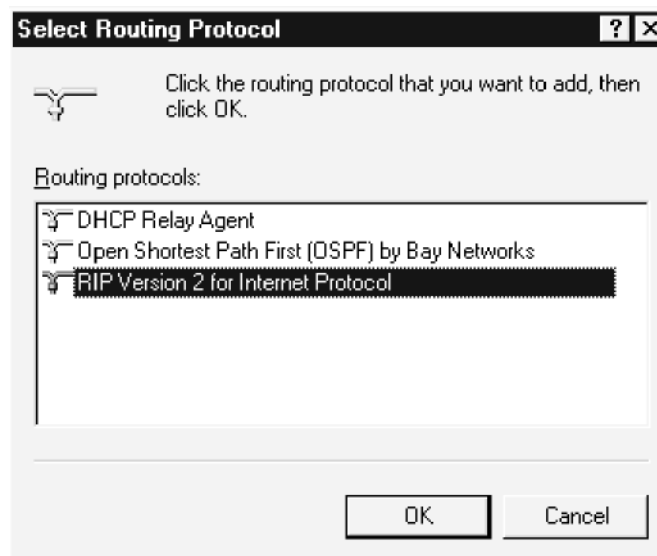
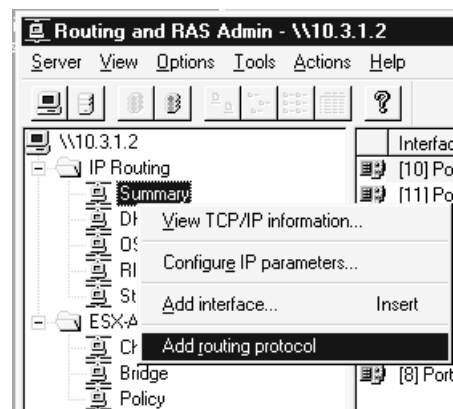
**Right-Click
on Summary
Icon**

**Select Add
Routing
Protocol**

Select RIP

In the Tree View:

1. Select the check box next to the IP Routing icon to display the Summary icon.
2. Right-click on the Summary icon to display a popup window.
3. Select the Add routing protocol menu item to display a dialog box.
4. Select RIP Version 2 for Internet Protocol to display the RIP for Internet Protocol Configuration page.



7.3.2 Configure the RIP Protocol

After adding the RIP protocol, configure RIP by performing the following tasks:

- Set RIP Protocol Parameters
- Limit Announcements to Trusted Neighbors

Set RIP Protocol Parameters

This procedure describes how to set the RIP protocol parameters that control how often updates are sent when the network topology is changing and determine the type of events that are logged.

On RIP for Internet Protocol Configuration page

Access the General Tab page

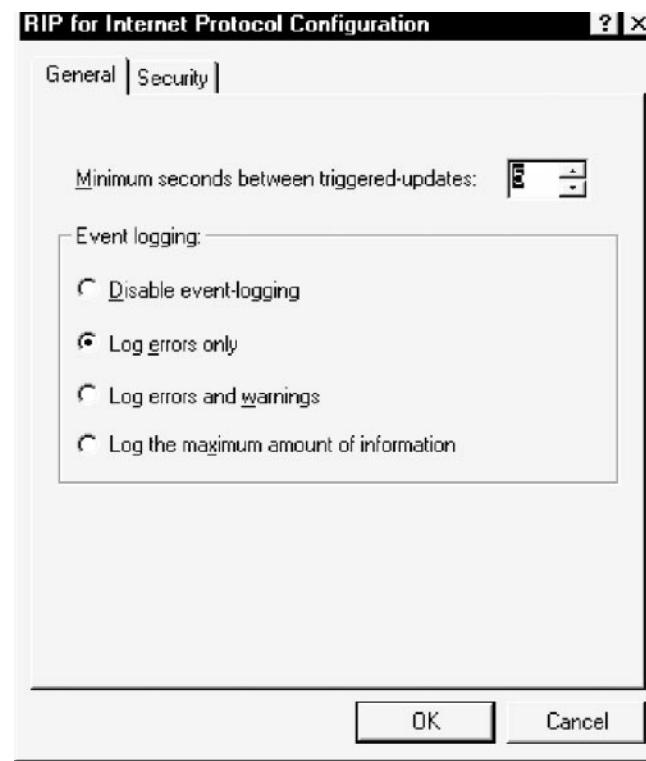
Set Triggered Update Frequency

Select Events for Logging

Click OK

On the RIP for Internet Protocol Configuration page:

1. Access the General tab page.
2. Select the triggered update frequency using the scrolling window.
3. Click a radio button to select the type of events that you want written to the log file.
4. Click OK to have the information take effect.



The example shows the triggered-update frequency and event logging parameters:

<u>Parameter</u>	<u>Value</u>
Seconds between triggered updates	Click the scroll bars to select a time value.
Event logging	Select logging options by clicking radio buttons.

Limit Announcements to Trusted Neighbors

This page is used to limit announcements to trusted neighbors.

On RIP for Internet Protocol Configuration page

Select Security Tab

Select Announcement Processing Method

Enter Router ID

Click Add

Click OK

On the RIP for Internet Protocol Configuration page:

1. Select the Security tab.
2. By clicking a radio button, choose one of these options:
 - process announcements from all routers
 - process announcements only from the routers listed
 - discard announcements from the routers listed
3. Enter the router IP interface address (if you selected the 2nd or 3rd option).
4. Click Add.

Note: The information you add will appear in the Routers: box.
5. Click OK to have the information in the Routers: box take effect.

RIP for Internet Protocol Configuration [?] [X]

General | **Security**

This page allows you to list the routers whose announcements should be processed or discarded.

☐ Process announcements from all routers.
☒ Process only announcements from the routers listed.
☐ Discard all announcements from the routers listed.

Routers:

101.237.85.1
101.237.85.17
101.237.85.9

Add Replace Delete

Router: [- - -]

OK Cancel

Click the ? icon in the menu bar and click on a field to access online help.

7.3.3 Set the Router's Interface Parameters

After adding the RIP protocol and configuring it, set the router's interface parameters by performing the following tasks:

- Define the Interface's Attributes
- Define the Routes the Interface Will Process
- Define the Interface's Neighbors
- Set the Interface's Timing Parameters

Define the Interface's Attributes

Defining a RIP interface's attributes is a two-step process:

- Choose an interface and access the RIP Configuration page
- Configure the interface's attributes

To choose an interface and access the RIP Configuration page:

In Tree View

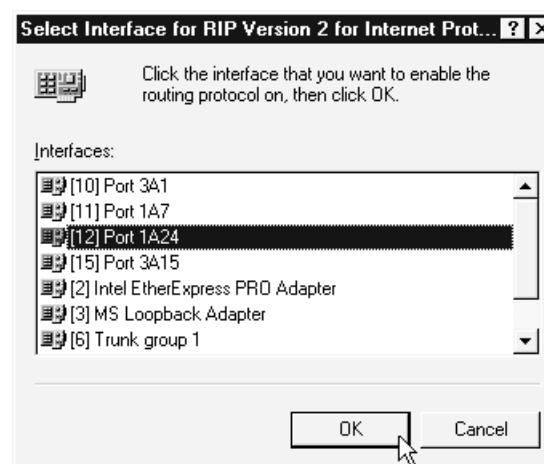
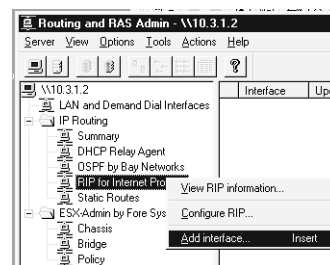
**Right-Click
OSPF by Bay
Networks**

**Select Add
Interface**

**Select an
Interface**

In the Tree View:

1. Right click next to the RIP icon to display a pop-up window.
2. Select the Add interface item to display the Select Interface for RIP window.
3. Select an interface you would like to add to RIP. The RIP configuration screen will appear, showing the port number of the interface on top.



Note: If you want to manage the switch over the RIP network, you will need to:

- Assign an IP address to adapter 3—see *Section 4.2, "Startup Sequence"* for details.
- Configure adapter 3's interface, the internal IP address of the switch, to run the RIP protocol as described in this section.

Define the Interface's Attributes (continued)

To configure the interface's attributes, follow this procedure:

**On RIP
Configuration
page**

**Set the
Interface's
Attributes**

Click OK

On the RIP Configuration page:

1. Set the interface's attributes, including:
 - Operation (update) mode
 - Version of RIP to use for outgoing and incoming updates
 - Route cost and tag information
 - Password
2. Click OK when you are finished, adding the new interface to RIP.

Note: Before clicking OK, access the Security, Neighbors, and Advanced tabs on the RIP Configuration page and perform the tasks in the following sections to:

- Define the Routes an Interface will Process
- Define the Interface's Neighbors
- Set the Interface's Timing Parameters

RIP Configuration - [14] Port 1A11

General | Security | Neighbors | Advanced

Operation mode: Periodic update mode

Protocol for outgoing packets: RIP version 1 broadcast

Protocol for incoming packets: RIP version 1 and 2

Added cost for routes using this interface: 1

Tag for routes advertised on this interface: 0

☐ Enable authentication

Password:

OK Cancel

The example shows the default values.

See online help for details. Click the ? icon in the menu bar and click on a field to access online help for that field.

Define the Routes the Interface Will Process

Define the the routes that a RIP interface will processes or ignore on the Security tab page by specifying a range of IP addresses.

**On RIP
Configuration
Page**

**Select Security
Tab**

**Specify Route
Processing
Option**

**Specify the
Range**

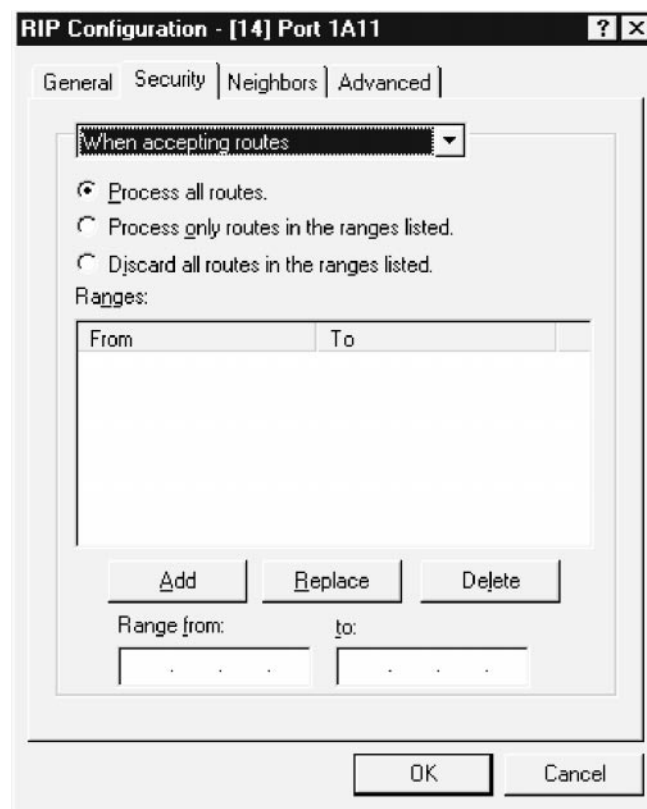
Click Add

Click OK

On the RIP Configuration page:

1. Select the Security tab, displaying the Security page.
2. By clicking a radio button, choose one of these options:
 - process all routes
 - process only routes in ranges listed
 - discard all routes in the ranges listed.
3. Specify the range, by entering a starting point and an end point for the range– a “from address” and a “to address”.
4. Click Add.

Note: The information you add will appear in the Ranges: box.
5. Click OK to have the information in the Ranges: box take effect.



Click the ? icon in the menu bar and click on a field to access online help.

Define the Interface's Neighbors

Select the Neighbors tab to define the interface's neighbors.

**On RIP
Configuration
Page**

**Select
Neighbors Tab**

**Specify
Neighbor
Option**

**Specify the
Neighbor's ID**

Click Add

Click OK

On the RIP Configuration page:

1. Select the Neighbors tab, displaying the Neighbors tab page.
2. By clicking a radio button, choose one of these options:
 - disable neighbor's list
 - use neighbor-list in addition to broadcast/multicast
 - use neighbor-list instead of broadcast/multicast
3. Specify the neighbor's ID (if you selected the 2nd or 3rd option).
4. Click Add

Note: The information you add will appear in the Neighbors: box.
5. Click OK to have the information in the Neighbors: box take effect.

RIP Configuration - [14] Port 1A11

General | Security | **Neighbors** | Advanced

This page lets you specify neighboring routers for RIP.

☒ **Disable neighbor-list**
☐ Use neighbor-list in addition to broadcast or multicast
☐ Use neighbor-list instead of broadcast or multicast

Neighbors:

Add Replace Delete

Neighbor: . . .

OK Cancel

Click the ? icon in the menu bar and click on a field to access online help.

7.3 Configuring RIP

Chapter 7 Configuring IP Routing and Protocols

Set the Interface's Timing Parameters

Access the Advanced tab to set timers and routing protocol options for RIP. The default parameters are shown in the example.

**On RIP
Configuration
Page**

**Select
Advanced Tab**

**Set Timer
Options**

**Set Protocol
Options**

Click OK

On the RIP Configuration page:

1. Select the Advanced tab, displaying the Advanced tab page.
 2. Set the timer options for:
 - announcement frequency
 - route expiration
 - route removal
 3. Set the protocol options.
2. Click OK to have the settings take effect.

The screenshot shows the 'RIP Configuration - [14] Port 1A11' dialog box with the 'Advanced' tab selected. The 'Timers' section contains three spinners: 'Periodic-announcement timer' set to 30, 'Route-expiration timer' set to 180, and 'Route-removal timer' set to 120. The 'Protocol options' section contains several checkboxes: 'Enable split-horizon processing' (checked), 'Enable poison-reverse processing' (checked), 'Enable triggered-updates' (checked), 'Send clean-up updates when stopping' (checked), 'Override non-RIP routes with RIP-learned routes' (unchecked), 'Process host routes in packets received' (unchecked), 'Include host routes in packets sent' (unchecked), 'Process default routes in packets received' (unchecked), and 'Include default routes in packets sent' (unchecked). The 'OK' and 'Cancel' buttons are at the bottom right.

The example shows the default values.

See online help for details. Click the ? icon in the menu bar and click on a field to access online help.

7.3.4 View RIP Information

Follow the information in this section to display RIP information:

In Tree View

Select RIP Icon

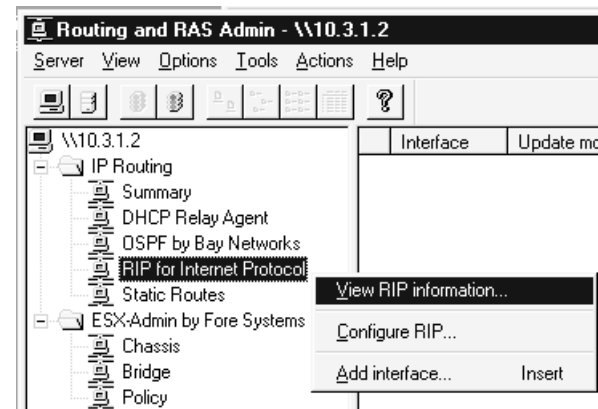
In Tree View

**Right-Click to
Display
Popup**

**Select
View RIP
Information**


In the Tree View:

1. In Tree View, select the RIP for Internet Protocol icon.
2. In the Tree view, right click to display the popup window.
3. Click the view selection to access the RIP Neighbors display described on the following page.



RIP Neighbors

The RIP Neighbors display shows parameter values for the RIP example.



Address	Version	Bad packets	Bad routes
---------	---------	-------------	------------

Ready

<u>Parameter</u>	<u>Description</u>
Address	The IP interface address of each neighbor.
Version	The RIP Version (Version 1 or Version 2) being run on the neighbor.
Bad packets	The cumulative number of packets that were received from neighbors with errors.
Bad routes	The cumulative number of routes received in updates which were in error.

7.4 Configuring Static Routes

You can assign a static route to a destination by directly specifying the IP address for the route, rather than by allowing a routing protocol to learn the route. This section describes the tasks to perform in order to configure a static route:

- Add a Static Route to an Interface 7.4.1
- View Static Route Information 7.4.2

7.4.1 Add a Static Route to an Interface

Use the Static Route screen to add a static route to an interface. Access the Static Route screen from the tree view.

In Tree View

**Right-Click
Static Routes
Icon**

**Select Static
Routes Menu
Item**

**Specify Static
Route
Parameters**

Click OK

In the Tree View:

1. Right click the Static Routes icon, displaying a popup menu.
2. Select the Static Routes Menu Item, displaying the Static Route screen.
3. Modify the Static Route page.
4. Click OK to add the static route.

The screenshot shows a 'Static Route' dialog box with the following fields and values:

- Destination:** 101.237.17.9
- Network mask:** 255.255.255.0
- Gateway:** 10.15.30.1
- Metric:** 1
- Interface:** [10] Port ???

Buttons: OK, Cancel

The example shows these Static Route parameters:

<u>Parameter</u>	<u>Value</u>
Destination	Dotted decimal number of the route destination.
Network Mask	Dotted decimal number of the contiguous mask.
Gateway	Destination IP address of next hop router used to reach this destination. Note: The interface must be able to reach the gateway, directly.
Metric	Cost associated with the route.
Interface	Hardware interface where gateway resides.

7.4.2 View IP Route Information (IP Routing Table)

Follow the information in this section to display the IP routing table:

In Tree View

**Select Static
Routes Icon**

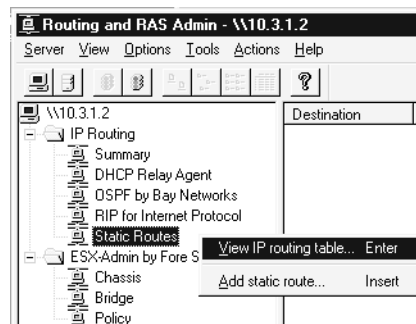
In Tree View

**Right-Click to
Display
Popup**

**Select View IP
Routing Table**

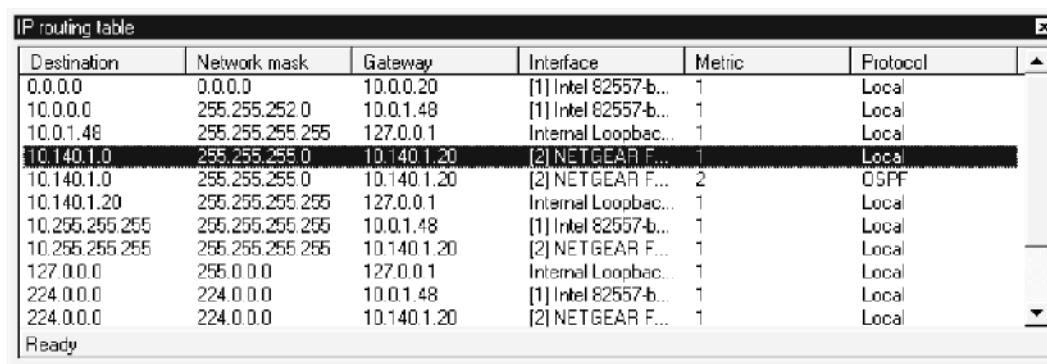
In the Tree View:

1. In Tree View, select the Static Routes for Internet Protocol icon.
2. In the Tree view, right click to display a popup window.
3. Click the view selection to display the IP routing table described on the following page.



View IP Route Information (IP Routing Table)

The IP routing table contains the addresses of the destination network and the next hop router. It also contains other information that may be helpful when you are checking the operational performance of the switch.



Destination	Network mask	Gateway	Interface	Metric	Protocol
0.0.0.0	0.0.0.0	10.0.0.20	[1] Intel 82557-b...	1	Local
10.0.0.0	255.255.252.0	10.0.1.48	[1] Intel 82557-b...	1	Local
10.0.1.48	255.255.255.255	127.0.0.1	Internal Loopbac...	1	Local
10.140.1.0	255.255.255.0	10.140.1.20	[2] NETGEAR F...	1	Local
10.140.1.0	255.255.255.0	10.140.1.20	[2] NETGEAR F...	2	OSPF
10.140.1.20	255.255.255.255	127.0.0.1	Internal Loopbac...	1	Local
10.255.255.255	255.255.255.255	10.0.1.48	[1] Intel 82557-b...	1	Local
10.255.255.255	255.255.255.255	10.140.1.20	[2] NETGEAR F...	1	Local
127.0.0.0	255.0.0.0	127.0.0.1	Internal Loopbac...	1	Local
224.0.0.0	224.0.0.0	10.0.1.48	[1] Intel 82557-b...	1	Local
224.0.0.0	224.0.0.0	10.140.1.20	[2] NETGEAR F...	1	Local

Ready

The IP routing table displays the following parameters:

<u>Parameter</u>	<u>Description</u>
Destination	Address of the destination network.
Network mask	The network mask of the destination network.
Gateway	Address of the next hop router.
Interface	Type of device attached to the interface.
Metric	Cost of the route.
Protocol	Protocol route was learned from.

7.5 Configure DHCP

You can add DHCP (Dynamic Host Configuration Protocol) to the switch and add a route to a DHCP server that will assign IP addresses to stations in the network by following the two-part procedure described in this section:

- Add DHCP
- Add a route to a DHCP server

To add DHCP:

In Tree View

Select IP
Routing Icon
Check Box

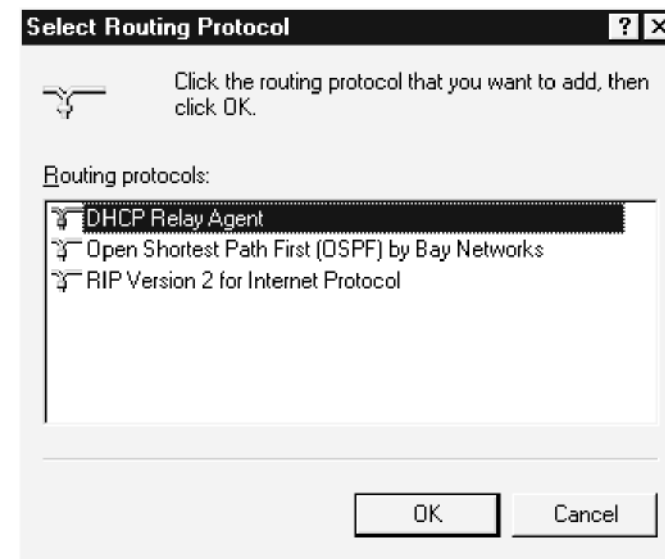
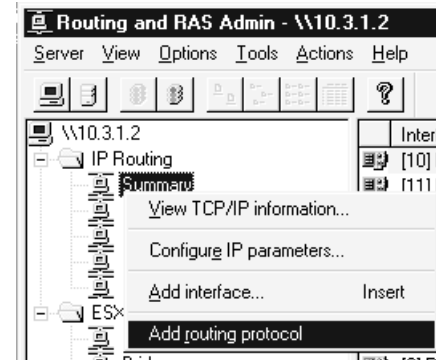
Right-Click
on Summary
Icon

Select Add
Routing
Protocol

Select DHCP
Relay Agent

In the Tree View:

1. Select the check box next to the IP Routing icon to display the Summary icon.
2. Right-click on the Summary icon to display a popup window.
3. Select the Add routing protocol menu item to display a dialog box.
4. Select DHCP Relay Agent to display the DHCP Relay Agent Configuration page.



Add a Route to a DHCP Server

This procedure describes how to add a path to a DHCP Server.

**On DHCP
Relay Agent
Configuration
Page**

**Enter the
Address of the
Server**

Click Add

Click OK

On the DHCP Relay Agent Configuration page:

1. Enter the address of the DHCP server in the Server: box.
2. Click Add.
3. Click OK to have the information take effect.

The screenshot shows the 'DHCP Relay Agent Configuration' dialog box with the 'General' tab selected. The 'DHCP Servers:' list contains the entry '1.1.1.1'. Below the list are 'Add' and 'Remove' buttons. At the bottom, the 'Server:' field is set to '1 . 1 . 1 . 1'. The 'OK' and 'Cancel' buttons are at the bottom right.

DHCP Servers:	
1.1.1.1	

Buttons: Add, Remove

Server: 1 . 1 . 1 . 1

Buttons: OK, Cancel

By setting up trunk groups, you can increase bandwidth and provide backup in the event an interface goes down. Follow the instructions in this chapter to select and configure ports on the switch as members of a trunk group.

When you configure ports as a trunk group, they appear to the switch as if they were a single logical port. When the switch receives packets, they appear to the switch as if they were coming from a single port. When the switch sends packets to a trunk group, it distributes traffic sessions equally among the trunked ports—based on a combination of the link that the packet was received on and the destination address.

You can configure both bridging and routing interfaces on a trunk group. The switch uses the MAC destination address to distribute bridge traffic, and it uses the IP destination address to distribute routed traffic.

This chapter contains the following sections that will guide you in configuring a trunk group:

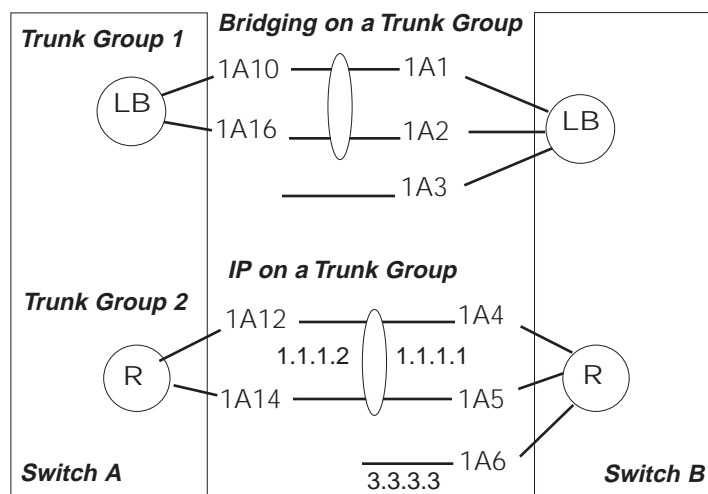
- 8.1 Trunking Overview
- 8.2 Creating a Trunk Group
- 8.3 Adding Ports to a Trunk Group
- 8.4 Removing Ports from a Trunk Group
- 8.5 Deleting a Trunk Group
- 8.6 Configuring Bridging on a Trunk Group
- 8.7 Configuring IP on a Trunk Group

8.1 Trunking Overview

A trunk group forms a single, logical pipe between two devices. As shown in the following diagram, you can set up bridging and IP on a trunk group just like you can set up bridging and IP on a port.

- **Bridging**—a trunk group on switch A (ports 10 and 16) is connected to a trunk group on switch B (ports 1 and 2)
- **IP**—a trunk group on switch A (ports 12 and 14) connects to a trunk group on switch B (ports 4 and 5).

Note: Ports 12 and 14 share one IP address (1.1.1.2). Ports 4 and 5 share another IP address (1.1.1.1) on the same subnet.



Example: Configuring Bridging and IP on Trunk Groups

You can configure both bridging and IP on the same trunk group. You can assign up to 16 ports to a trunk group and you can establish up to 16 trunk groups on a single switch.

Note: You can connect devices to the ports that you designate as members of a trunk group either before or after you configure the trunk group.

Glossary




Bridge A communication device that connects two or more networks and selectively forwards packets between them using the physical layer (layer 2 in the OSI model).

Learning Bridge A bridge that learns the addresses of devices and hosts connected to the bridge group and forwards packets to a device directly, once it has learned its address, rather than broadcasting the packets to all the devices attached to the bridge.

Router A computer that connects to two or more local area networks and forwards layer 3 datagrams from one to another. Using the destination address in the datagram, the router picks the next hop and forwards the datagram.

Trunk Group Two or more ports that are seen by the bridge or router as a single, logical port. When a bridge or router receives packets from a trunk group, it processes them as if they arrived on the same port. When it sends, it distributes the packets among the ports that make up the trunk group.

Legend:

-  **Learning Bridge**
-  **Router**
-  **Trunk Group**

Link Failure and Recovery

When links belonging to a trunk group go down and come back up, the switch automatically senses which ports in the trunk group are live and rebalances the traffic among them, accordingly.

8.1 Trunking Overview continued

Bridging Traffic between Three Switches Using Trunking

Using the switch, you can establish a bridged trunk connection between two other switches.

The following diagram shows three switches connected by two trunk groups that belong to the same bridge group:

- Trunk Group 1 connects Switch A and Switch B.
- Trunk Group 2 connects Switch A and Switch C.

To implement this example,

1. Set up Trunk Groups 1 and 2 on Switch A

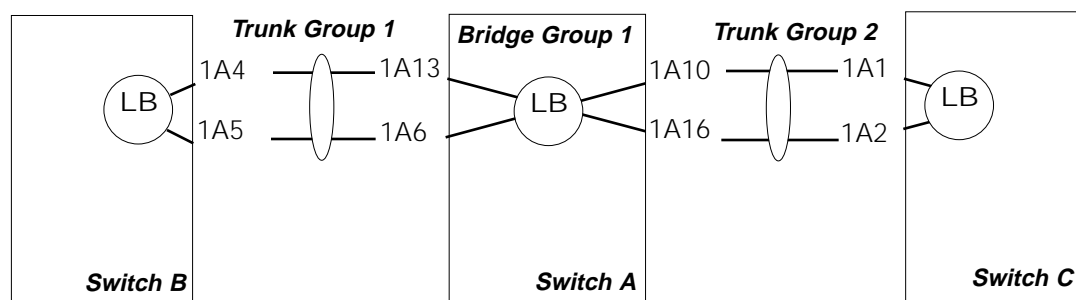
2. Create Bridge Group 1 on Switch A and add both Trunk Group 1 and Trunk Group 2 to Bridge Group 1.

3. Repeat Steps 1 and 2 for Switches B and C.

Trunking a FORE Systems ESX Switch with other Vendor Equipment

You can connect bridged trunks between FORE Systems switches and switches from other vendors. Refer to the vendor requirements when setting up the trunk groups on other vendor equipment.

Note: Other vendor equipment may require you to set up a trunk using consecutive port numbers. As shown in the diagram, this is not a requirement for FORE Systems ESX switches.



Example: Bridging traffic between Three Switches Using Trunking

8.2 Creating a Trunk Group

You can create a trunk group and add ports to the trunk group by following this two-part procedure:

- Select a port or group of ports
- Select the Create Trunk Group menu item

Note: You can create up to 16 trunk groups on a single switch and up to 16 ports in a single trunk group.

In Display View

Select a Port or Group of Ports

Right Click and Select Editing Mode

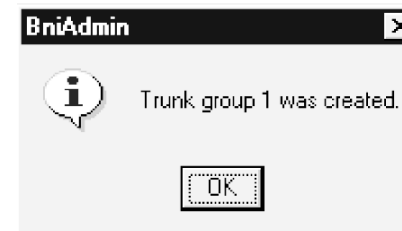
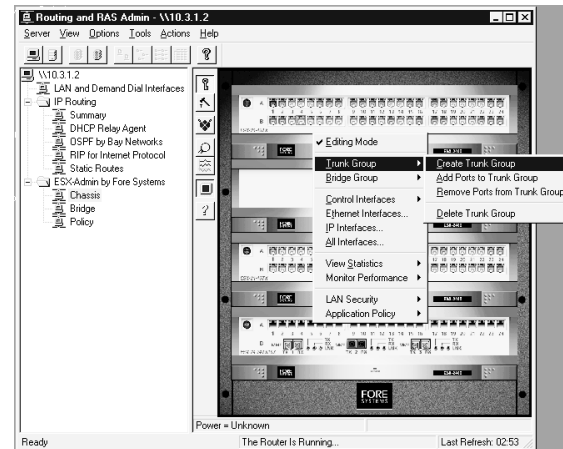
Right Click and Select Trunk Group & Create Trunk Group

In the Display View:

1. Select a port or group of ports.
2. Right Click in Display View and select Editing Mode.
3. Right Click again in Display View and select Trunk Group and Create Trunk Group to create a trunk group with the ports you selected in step 1 as members of the trunk group.

Note: After you create the trunk group, a message will appear on the screen confirming that the trunk group was created. When you position your cursor on a port the number of the trunk group it belongs to is displayed in a message box.

Caution: Do NOT connect the NSC control port to a trunk group.



To select multiple consecutive ports:

When configuring ports on the switch you may want to select multiple ports and configure them identically. To select multiple, consecutive ports, press the CTRL key while you hold down the left mouse button activating a lasso, and use the lasso to select multiple consecutive ports.

8.3 Adding Ports to a Trunk Group

You can add ports dynamically to an existing trunk group. When you add new ports to a trunk group, the switch will automatically rebalance the traffic among the ports in the trunk group. To add ports to a trunk group:

In Display View

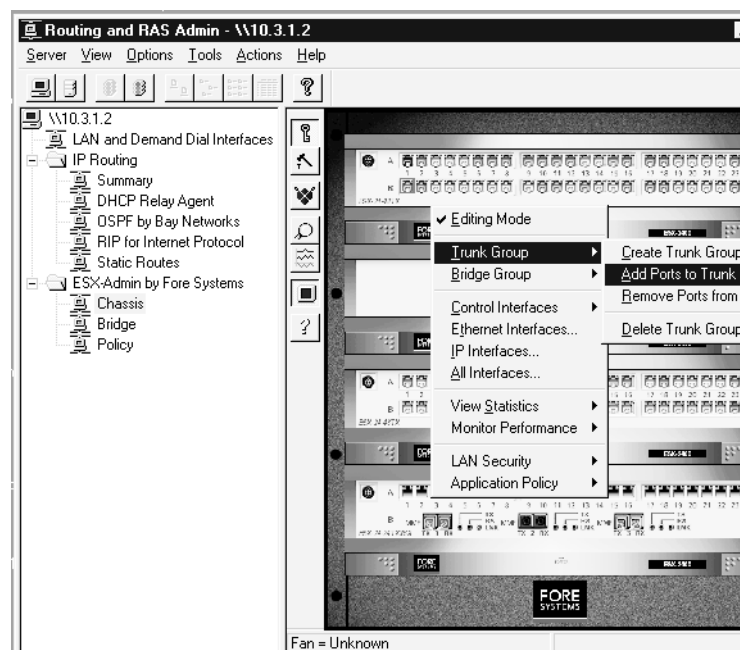
Select a Port or Group of Ports

Right Click and Select Editing Mode

Right Click and Select: Trunk Group, Add Ports to Trunk Group, and Trunk Group Number

In the Display View:

1. Select a port or group of ports you want to add to a trunk group.
2. Right click to display the Edit Mode pop-up menu and select Editing Mode.
3. Right Click again in Display View to access the Editing Mode popup and select:
 - Trunk Group
 - Add Ports to Trunk Group
 - Trunk Group Number



Link Failure and Recovery

When links belonging to a trunk group go down and come back up, the switch automatically senses which ports in the trunk group are live and rebalances the traffic among them, accordingly.

8.4 Removing Ports from a Trunk Group

When you remove ports from an existing trunk group, the switch automatically rebalances the traffic among the remaining ports in the trunk group. To remove ports from a trunk group:

In Display View

Select a Port

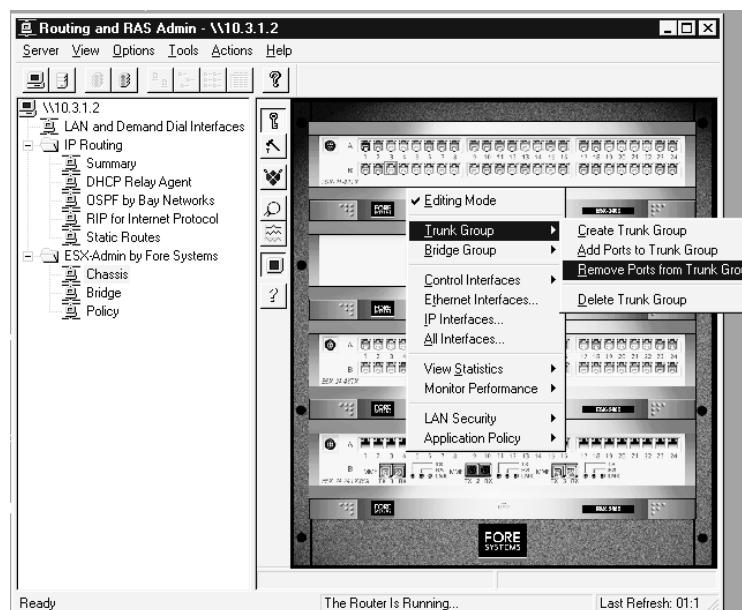
Right-Click and Select Editing Mode

Right-Click and Select: Trunk Group, Remove Ports from Trunk Group, and Trunk Group Number

In the Display View:

1. Select a port or group of ports you wish to remove from a trunk group.
2. Right click to display the Edit Mode pop-up menu and select Editing Mode.
3. Right-click again in Display View to access the Editing Mode popup and select:
 - Trunk Group
 - Remove Ports from Trunk Group

Note: A message will appear on the screen confirming that ports were removed from a trunk group.



Link Failure and Recovery

When links belonging to a trunk group go down and come back up, the switch automatically senses which ports in the trunk group are live and rebalances the traffic among them, accordingly.

8.5 Deleting a Trunk Group

To delete a trunk group:

**In Display
View**

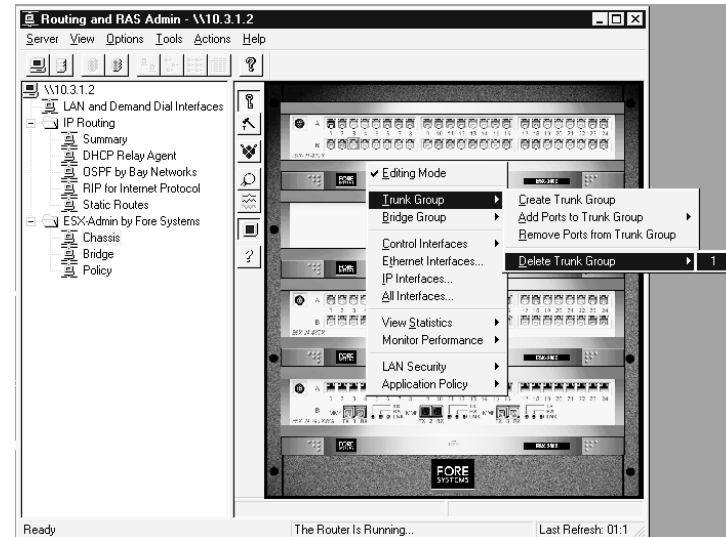
**Select a Port
or Group of
Ports**

**Right-Click
and Select
Editing Mode**

**Right-Click and
Select: Trunk
Group, Remove
Ports from
Trunk Group,
and Trunk
Group Number**

In the Display View:

1. Select a port or group of ports belonging to the trunk group you wish to delete.
2. Right-click in Display View and select Editing Mode.
3. Right-click again in Display View and select:
 - Trunk Group
 - Delete Trunk Group



8.6 Configuring Bridging on a Trunk Group

To configure bridging on a trunk group, after you create the trunk group, create a bridge group and add the trunk group to the bridge group.

See Chapter 6, Configuring Bridging for detailed information describing how to create a Bridge Group.

To create a bridge group and assign a trunk group to the bridge group:

In Tree View

Select Bridge Icon

In Display View

Select a Bridge Group

Right-Click to Display Popup

Select Create Bridge Group

Add Port to Bridge Group

In the Tree View:

1. Select the bridge icon.

In the Display View:

2. Select a bridge group.

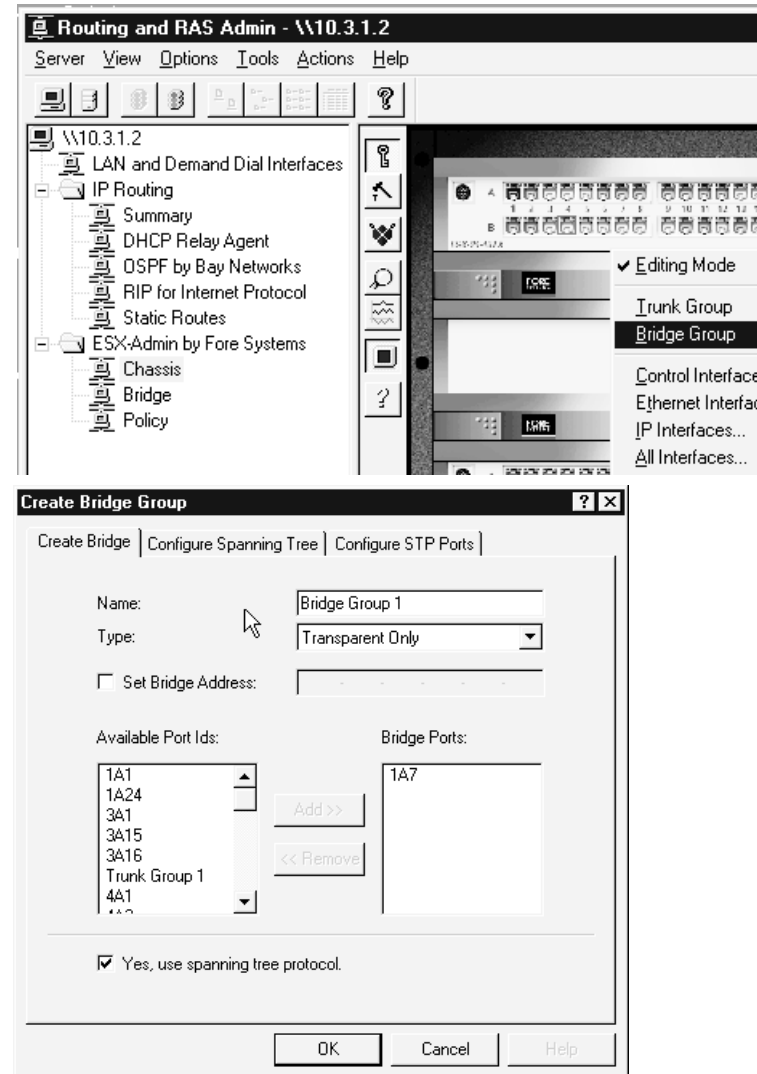
3. Right click to display a popup window.

4. On the popup window, select the Create Bridge Group page.

5. On the Create Bridge Group page:

- check the Available Port window
- select the trunk group
- click Add
- click OK

Note: You must create the trunk group before creating the bridge group.



8.7 Configuring IP on a Trunk Group

To configure IP on a trunk group, assign an IP address to a port in the trunk group. After an IP address is assigned to a port belonging to the trunk group all ports in the trunk group will use this IP address.

To assign an IP address to a port:

In Display View

Select Trunked Port

Right-Click to Display Edit Menu

Select IP Interfaces

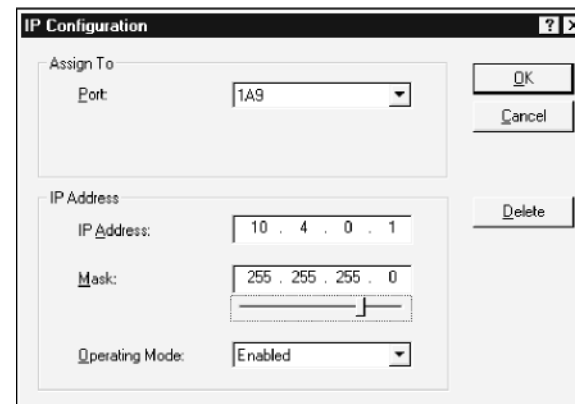
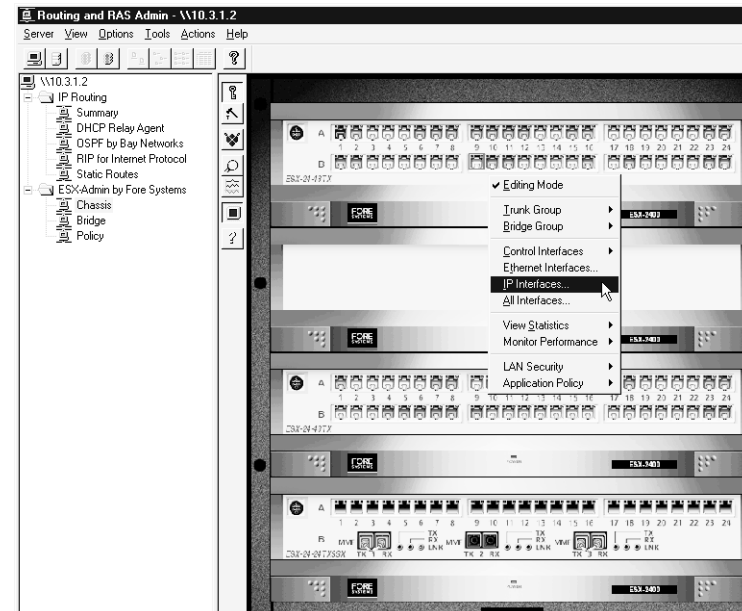
Enter IP Interface and Mask

Select Enabled

In the Display View:

1. Select a trunked port.
2. Right-click to display the Edit Mode pop-up menu.
3. Select the IP Interfaces menu item to display the IP Configuration page.
4. Enter the IP address and mask.
5. Select Enabled (default) to enable the IP address.

Note: When you assign an IP address to a trunk group, the switch enables IP routing on the trunk group.



This chapter describes how to monitor performance using ESX-Mon, the performance monitoring tool provided with the ESX-Vision software. It describes useful performance monitoring techniques, and it provides basic information to help you get started using ESX-Mon to monitor your switch. The information you can collect using ESX-Mon will help you manage the switch, balance the loads on your network, and perform capacity planning required to manage network growth.

- 9.1 Performance Monitoring Overview
- 9.2 Objects & Counters
- 9.3 Starting ESX-Mon
- 9.4 Displaying Counters
- 9.5 Printing a Window Display
- 9.6 Logging and Viewing Logs
- 9.7 Logging Errors to the Event Viewer

9.1 Performance Monitoring Overview

Using ESX-Mon, the performance monitoring tool supplied with the switch, you can display the type and the amount of traffic moving through your network, graphically.

Using the graphic information that ESX-Mon provides, you can:

- Identify bottlenecks that may exist
- Understand how traffic changes during the day
- Identify growth in the amount of traffic over time
- Develop effective plans to increase the capacity of your network to handle increased traffic loads

9.2 Objects and Counters

ESX-Mon is based on PerfMon, the performance monitoring tool supplied with Windows NT. ESX-Mon allows you to select and display objects and set counters associated with these objects on your management station.

FORE Systems supplies three object types and counters associated with these object types that allow you to measure and display the traffic moving through the switch graphically:

- ESX IP STATISTICS
- ESX ETHERNET
- ESX HOST STATISTICS

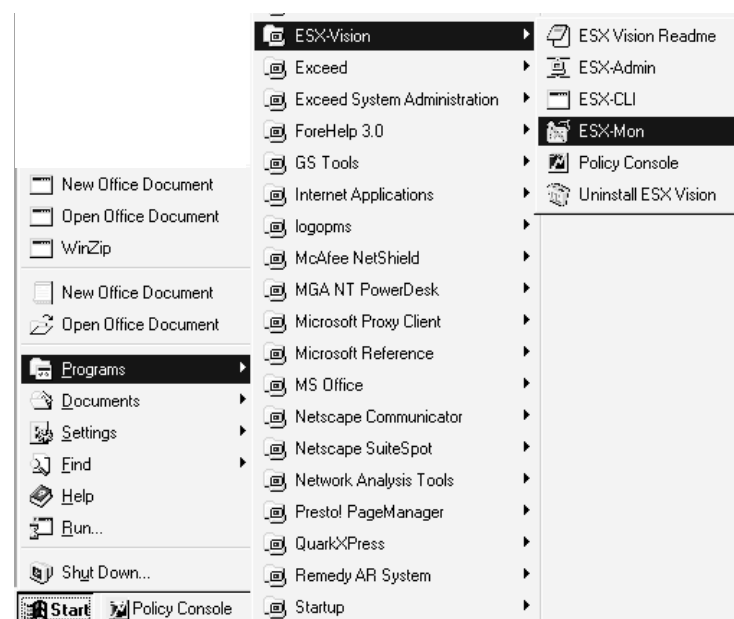
ESX-Mon allows you to view the same counters that you are able to view using the ESX-Admin facility. After you start the ESX-Mon facility and select an object, you can view that counter's objects in a scrolling window.

9.3 Starting ESX-Mon

You can access ESX-Mon either from the start menu or from within ESX-Admin.

To Start ESX-Mon from the Start Menu:

Select Programs, select ESX-Vision, then select ESX-Mon:



9.3 Starting ESX-Mon

Chapter 9 Performance Monitoring

To Start ESX-Mon from ESX-Admin

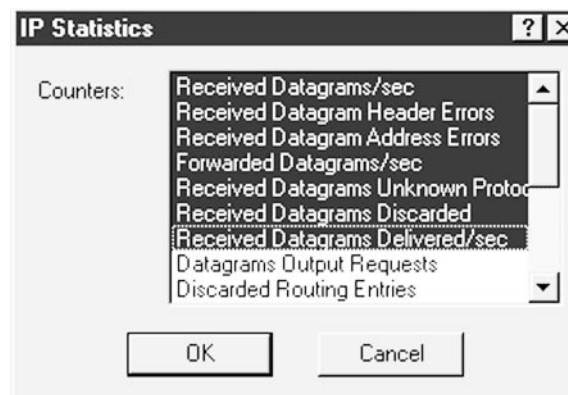
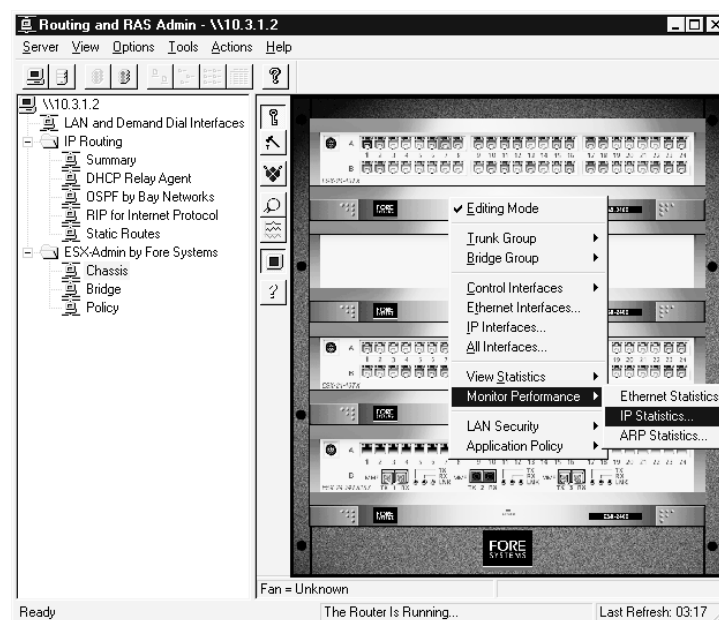
Once you have started ESX-Admin, you can start ESX-Mon by following this procedure:

In Tree View:

1. Select the Chassis icon.

In Chassis View:

1. Right click to display the Edit menu.
2. Select the Editing Mode menu item to activate editing mode.
3. Select a port or group of ports and right click to display the Edit menu again.
4. Select Monitor Performance and either Ethernet Statistics, IP Statistics, or ARP Statistics to display a statistics window. *If you selected IP statistics, the IP Statistics window will be displayed.*
5. Select the counters you would like to see displayed and click OK to display the Performance Monitor window shown on the following page.



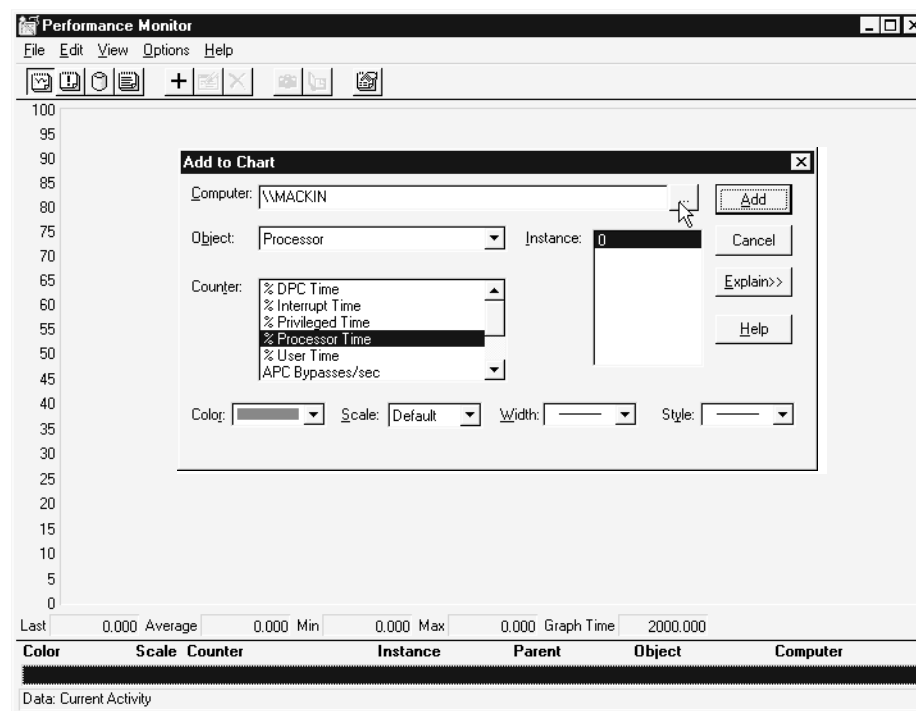
9.4 Displaying Counters

After you start ESX-Mon, the Performance Monitor window will appear along with an Add to Chart window.

Do not fill in information on the Add to Chart window.

Follow the instructions on the next page that describe how to select a computer and display counters.

Note: You can access online help for the Performance Monitor by pulling down the menu at the top of the Performance Monitor window.



Select a Computer to Monitor

Before you can select objects and display statistics collected by the counters you set on your screen, you need to select the computer you want to monitor.

Note: If your client machine and the switch are in different domains you need to build a session with the switch you want to monitor before using ESX-Mon. You can build a session using the ESX-Cli connect command, or with the netuse command in addition to ESX-Admin.

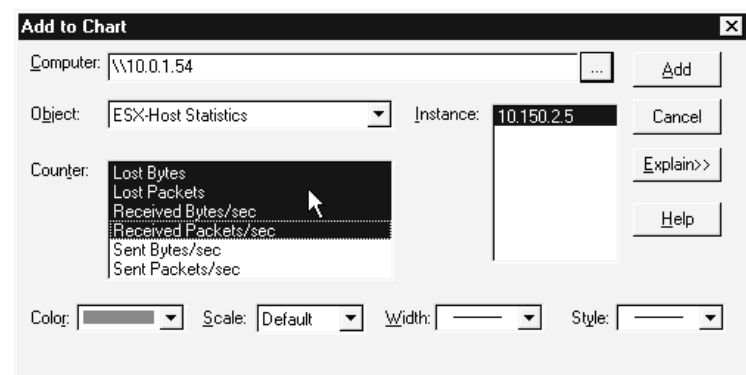
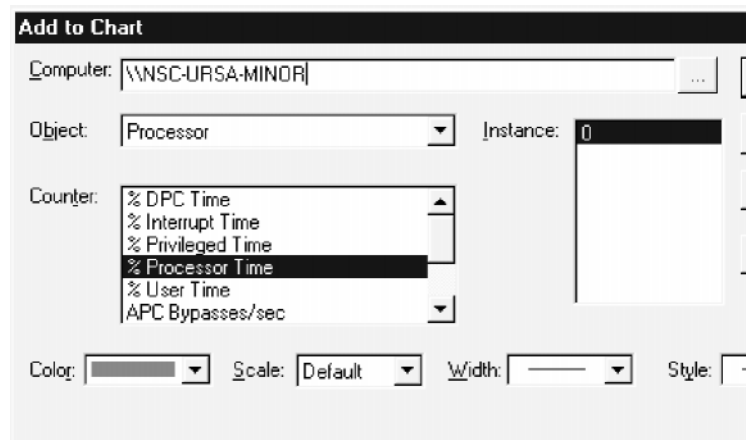
1. Click the plus [+] icon at the top of your screen to display the Add to Chart dialog box.
2. Enter the name of the computer you want to monitor in the Computer: field.

Select an Object and Add a Counter to the Chart

When you use ESX-Mon, you select an object and add one of its counters to the chart. You can add additional counters from the same object. You can also select additional objects and add counters for those objects.

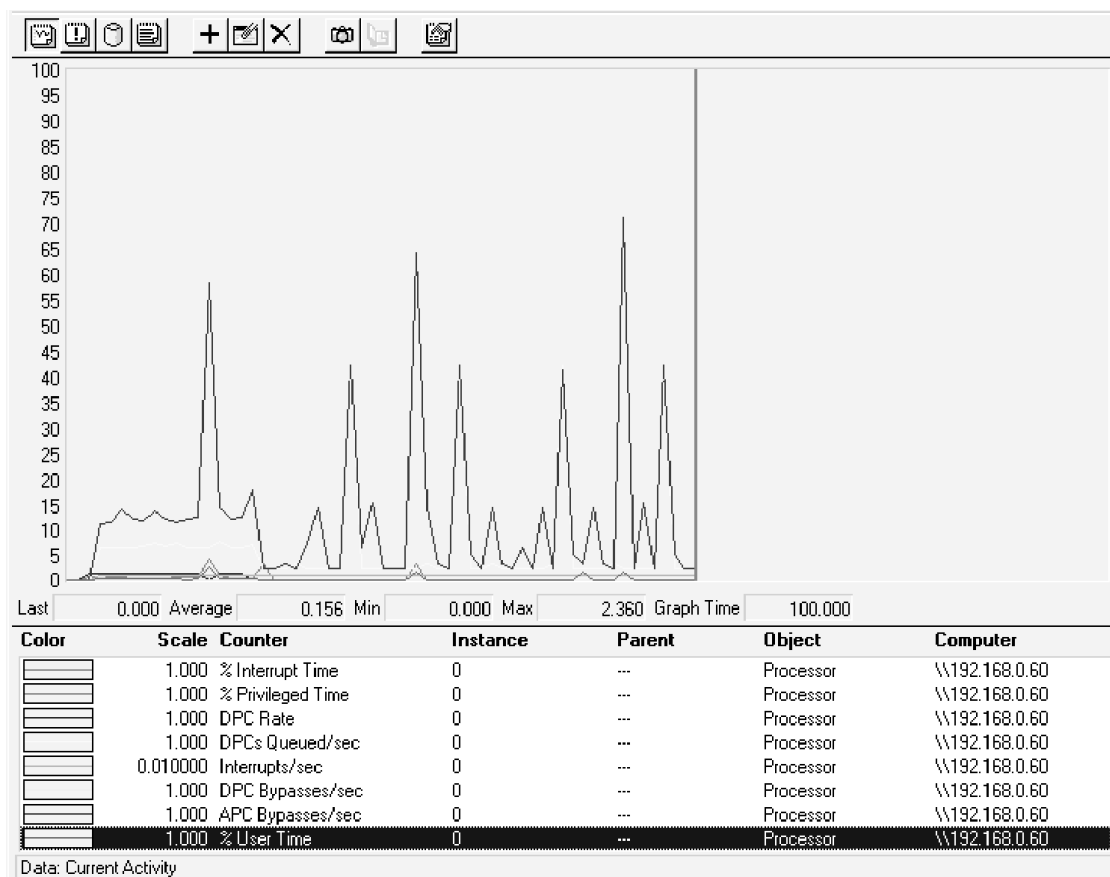
To select an object and add a counter for that object:

1. Click the plus [+] icon at the top of your screen to display the Add to Chart dialog box.
2. Select an object in the Object: pull down menu.
3. Select one of the object's counters in the Counter: pull down menu.
4. Click Add to display the statistics gathered by that counter, graphically, in the Performance Monitor window.



Performance Monitor Display

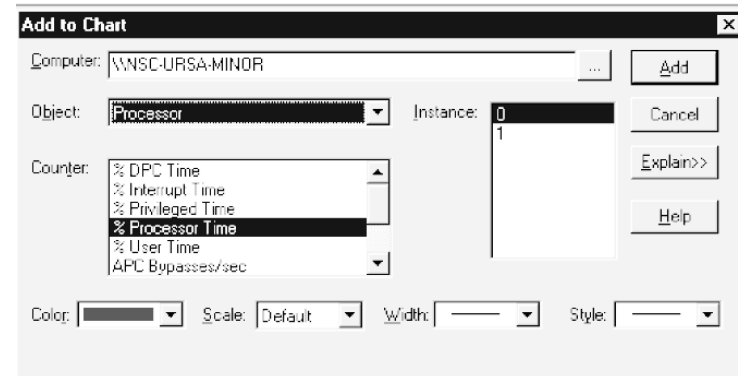
The following screen is an example of a Performance Monitor display:



Customize the Line Graphed for a Counter

You can customize the way ESX-Mon graphs lines on the screen. You can adjust color, width, and style for individual lines that ESX-Mon graphs. And you can adjust the vertical scale of the line that ESX-Mon graphs using pull down menus at the bottom of the Add to Chart menu.

Note: ESX-Mon uses a 20 sec interval for sampling the counters it graphs on the display.



9.5 Printing a Window Display

You can print a snapshot of the current window:

1. Press ALT + PRINT SCREEN to copy the active window to the clipboard.
2. Click Start, point to Accessories, and click Paint to open the Paint application.
3. Pull down the Edit menu and click Paste.
4. Click Print.

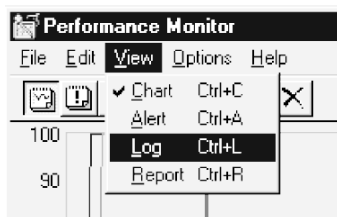
9.6 Logging and Viewing Logs

You can log counter statistics, rather than displaying them graphically on the screen. Later, you can open the log ESX-Mon created and display the log's contents, graphically, on the screen.

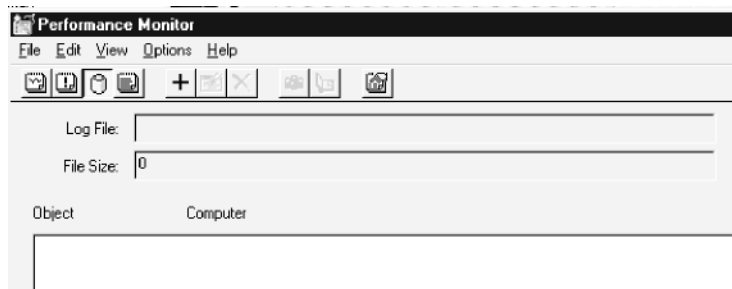
To Create a Log File:

On the Performance Monitoring window.

1. Pull down the View menu.

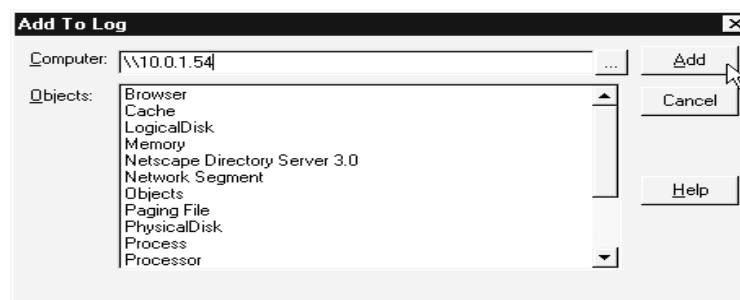


2. Select log to display log information inside the Performance Monitoring window.

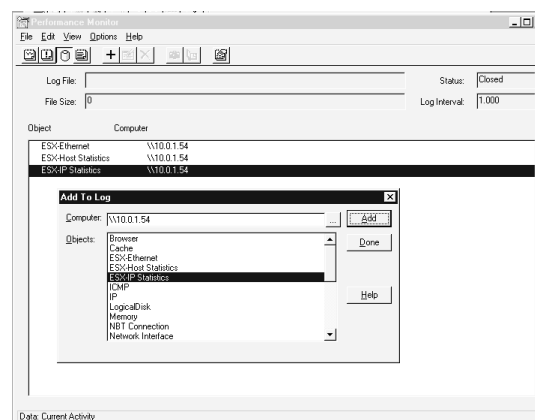


3. Click the [+] icon at the top of the Performance Monitoring window to display the Add to Log dialog box.

4. Click the [...] button, fill in the Computer: field with the name of the computer you want to monitor, and Click Add.



5. Select the objects you want to observe –ESX Ethernet, ESX IP Statistics, and ESX Host Statistics are supported.

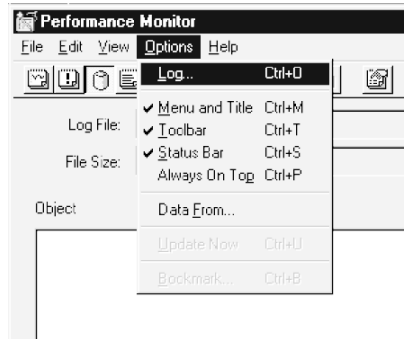


6. Click Add then click Done.

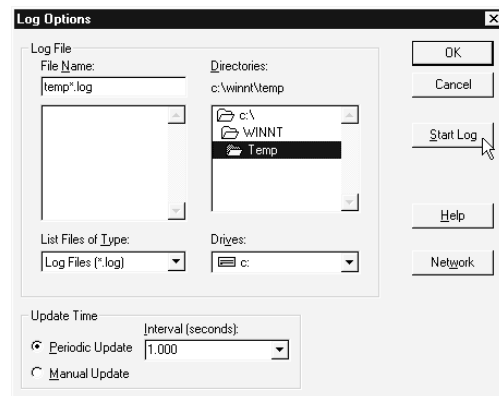
Note: ESX-Mon logs all object counters and all switch instances (ports or IP addresses) for the objects you select. When you chart the log file later, you can graph any of the counters for any of the ports or IP addresses on the switch.

To Create a Log File (continued)

7. Pull down the Options menu and select Log to display the Log Options dialog box.



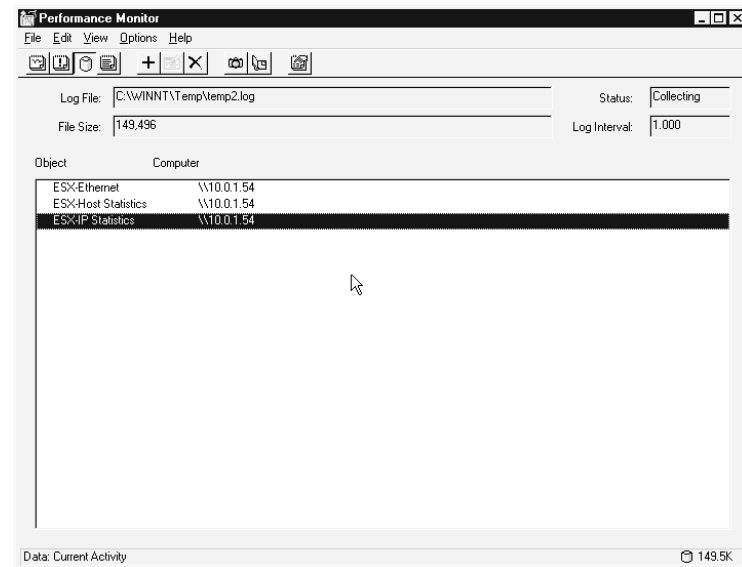
8. Enter a name in the File Name: field.
9. Specify a directory.
10. Set a time variable in seconds in the Periodic Update: field.



11. Click the Start Log button

Note: The log information displayed in the Performance Monitoring window will show:

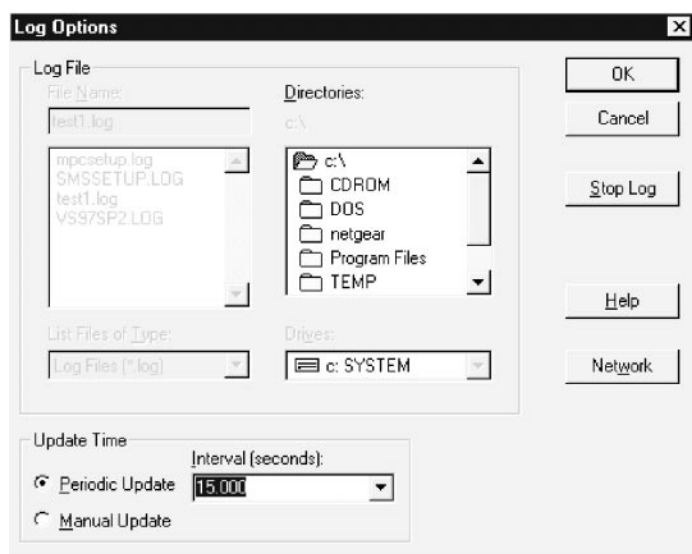
- The file name you specified
- The status will change to: Collecting
- The file size will grow as the file increases in size
- The log Interval will display the value you specified .



To Stop Logging to the Log File

On the Performance Monitoring window:

1. Pull down the Options menu and select Log to display the Log Options menu.
2. Click the Stop Logging button to stop logging.



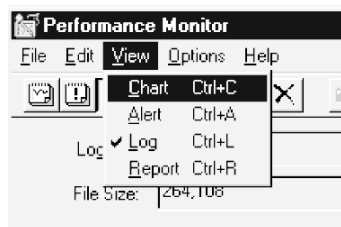
9.6 Logging and Viewing Logs

Chapter 9 Performance Monitoring

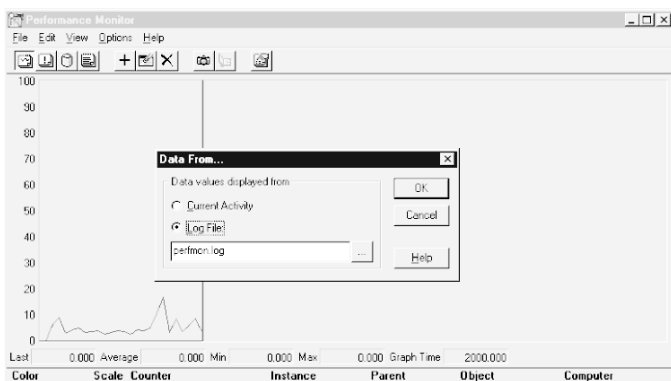
To View a Chart of Log File Data

On the Performance Monitoring window:

1. Pull down the View menu and select Chart.

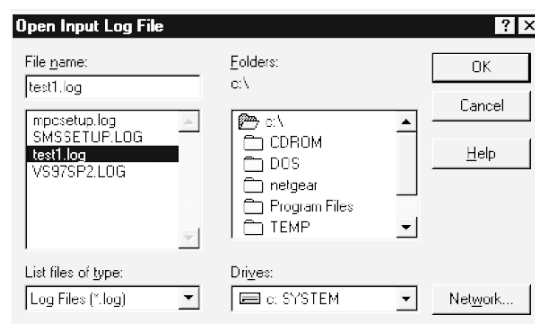


2. Pull down the Options menu and select Data From.



3. Click the Log File radio button..

4. Click the [...] button to the right of the file name field to display the Open Input Log File dialog box.

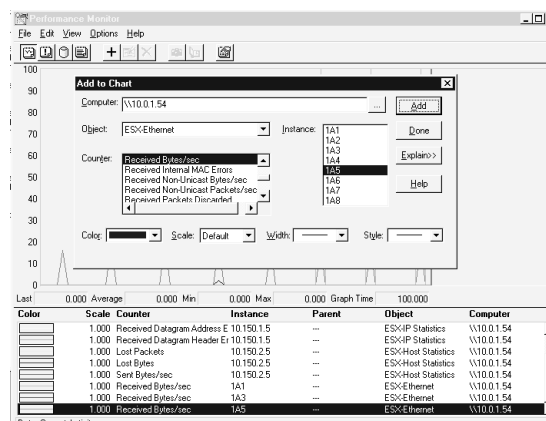


5. Select the file you want to chart and specify a directory.

6. Click OK on the Open Input Log File dialog box.

7. Click OK on the Data From dialog box to display the main Performance Monitor window.

8. Click the [+] icon on the top of Performance Monitoring window to display the Add to Chart dialog box.



9. Select the object, counter, and instance (port or IP address) you want to chart and click Add.

This chapter provides an overview of the troubleshooting process. It describes useful troubleshooting tools. And it contains step-by-step instructions to assist you in isolating and correcting switch and network problems. In the event you are unable to resolve a problem condition, this chapter describes how to contact FORE Systems Technical Support.

- 10.1 Troubleshooting Overview
- 10.2 Troubleshooting Tools
- 10.3 Startup and Hardware Problems
- 10.4 Ethernet Problems
- 10.5 Bridged Network Problems
- 10.6 TCP/IP Problems
- 10.7 SNMP Problems
- 10.8 Managing Disks and Reconstructing Arrays
- 10.9 Reporting Problems

10.1 Troubleshooting Overview

To troubleshoot your system effectively, you need to understand your system configuration and follow an effective problem solving approach. This section provides an overview of switch and network configuration—covered in detail in previous chapters. It also contains a problem solving checklist that can assist you in identifying switch and network-related problems.

<u>Topic</u>	<u>Section</u>
• Switch and Network Configuration	10.1.1
• Problem Solving Checklist	10.1.2

10.1.1 Switch and Network Configuration

When you perform the start-up sequence, described in Chapter 4, Startup, you begin configuring the switch. You continue configuring the switch, when you configure hardware, described in Chapter 5, Switch Configuration. You complete the configuration process when you configure your network—covered in Chapter 6, Configuring Bridging and Chapter 7, Configuring IP Routing and Protocols.

You can load the switch configuration to a file and restore the saved configuration by following the procedures described in the **ESX-Cli Command Console Guide**.

If you save the configuration to a file whenever you change the configuration, you can back out changes and restore stable operation, in the event changes to the configuration cause switch or networks problems.

10.1.2 Problem Solving Checklist

This checklist is provided to assist you in identifying switch or network-related faults.

Installation

- ☐ Check the indicators on the switch—see Chapter 2, “Installing the ESX-4800” or Chapter 3, “Installing the ESX-4800”.

Startup or Reboot

- ☐ Check your configuration settings and system indicators—see Chapter 4, “Startup”.

Post-Startup

- ☐ Check the indicators on the switch—see Chapter 2, “Installing the ESX-4800” or Chapter 3, “Installing the ESX-2400”.
- ☐ Check switch information—see Chapter 5, “Switch Configuration”, Chapter 6, “Configuring Bridging”, and Chapter 7, “Configuring IP Routing and Protocols”.
- ☐ Check any error messages provided by the system—see Chapter 5, “Switch Configuration” and Section 10.2.3, “NT Troubleshooting Tools”.
- ☐ Compare the current switch configuration to the original configuration—see the ESX-Cli **save** and **load** command descriptions in the **ESX-Cli Command Console Guide** for details.
- ☐ Check recent changes to the switch or network configuration.

10.2 Troubleshooting Tools

You can use tools provided with your system in order to isolate switch or network-related faults. This section provides an overview of these troubleshooting tools.

- 10.2.1 ESX-Cli Commands
- 10.2.2 dc Test
- 10.2.3 NT Troubleshooting Tools

10.2.1 ESX-Cli Commands

You can use the ESX-Cli Command Console to collect information and execute tests that will assist in isolating faults. See the **ESX-Cli Command Console Guide** for detailed information on the following ESX-CLI commands that are useful in troubleshooting:

Show Command

Use the **show** command to display statistics or configuration information about a subsystem.

10.2.2 dc Test

The dc Test, provides status information about the reliability of the hardware.

First, the dc test displays the hardware configuration, allowing you to compare what you have installed with what the system recognizes.

Next, the dc test sends and returns packets on each configured port. It reports any errors it detects, before removing any bad ports it finds from the test and resuming the test sequence.

The dc test executes until a predefined number of packets have been transmitted, or until you terminate testing using a command from the terminal.

1. dc Test Setup

Telnet to the NSC or connect a terminal or PC, locally, to the serial port of the NSC attached to the switch you want to test—for details, see Chapter 2, Installing the ESX-4800 or Chapter 3, Installing the ESX-2400.

Follow instructions in Section 4.2, “Startup”, to:

- Power on the terminal
- Logon to the NSC and obtain a DOS prompt

2. Starting the dc Test

Before you can execute the dc test, you need to stop the switch by issuing the ESX-CLI **stop** command.

1. At the CLI> prompt, enter:

```
stop
```

Note: This stops the normal operation of the switch

2. Either wait 60 sec. for the switch to reset, or force a reset by issuing the following commands at the the DOS prompt:

```
set com-port ether
reset lcp slot 1
exit
```

3. Enter:

```
cd c:\diagnostics\dc
```

4. At the CLI>prompt, enter:

```
dc
```

3. Stopping the dc Test

To stop the dc test, issue the **q** (quit) command, or set a specified number of packets that you want dc to transmit when you issue the dc command:

```
dc -n < # >
```

4. Interpreting the dc Test Results

Before the dc test executes, it displays the hardware configuration that it recognizes—see the sample dc Test output.

In the example, the dc Test recognizes 1 slot, Slot 1, and is testing ports 1a2 to 1a24. Port 1 is being used as the control port, which dc will not test.

When dc executes it will display the status every second—overwriting the display. When it detects errors on a port, a group of ports, or a slot, it will remove the failing element from the test and continue testing. When you stop the dc Test by entering **q** (quit), the last screen is redisplayed. This test was stopped when 3000 packets had been transmitted.

Note: If the display does not recognize a slot where you have installed hardware:

- Eject the card or module from the slot
- Reinsert it
- Run dc again
- Call Technical Support if dc fails to recognize a card or module after you have reseated it.

```

Slot SerNo Platf MB   MCA      MCB      LCP rev SE rev
-----
  1   1026 2400   10.0 24TX-1v11 3SX-8100 4.0.9   2.0

Average loopback load: 19.46% TX
(pkt size:60-1514 cycle:30 pkt/s:100 burst:1)

Connected port: 1a1

00:00:00 02:19:37 - Test started; Press 'q' to quit, '?' to display
test parameters

Testing ports: 1a2-1a24 1b*
Dropped ports: none

Transmitted          3000          Missing          0
Received             2985          Out of order       0
In flight             15           Corrupt            0
Max in flight         24           Corrupt pktid      0
Hello                 34           Bad length         0
Lcp message           0           Bad tag            0
Other                  0           Send error         0
Packet rate           100 pps
Loopback load         19.47 %
Packet size            889

00:00:30 02:20:07 - User exit

Testing ports: 1a2-1a24 1b*
Dropped ports: none

Transmitted          3051          Missing          0
Received             3051          Out of order       0
In flight              0           Corrupt            0
Max in flight         24           Corrupt pktid      0
Hello                  41           Bad length         0
Lcp message           0           Bad tag            0
Other                  0           Send error         0
Packet rate            99 pps
Loopback load         19.46 %
Packet size           1106

```


5. Examining the dc Test Results

If errors occur, when you execute the dc Test, dc opens a file in the current directory, and writes the test results to that file

The default location where the file will be written is the root for the C: drive. You can change this location with the -logdir command line option.

An example of a dc Test file name follows:

2400_00123_1998-05-09_15-29-56.txt

chassis type ser# date time file type

Note: when it writes the test file, the dc Test specifies your chassis type in the file name, either: 2400 or 4800

6. Saving the Test File

By default, the dc Test saves the test results only if test failures are detected. Run the dc test with this option: **dc -keepfile yes** to change the default setting.

7. Sending dc Test Results to FORE Systems

While troubleshooting your system, you may need to send the dc test file to FORE Systems. You can attach the test file to a mail message and send the message to:

Support@FORE.com

```

Slot SerNo Platf MB      MCA      MCB      LCP rev  SE rev
-----
1    1026   2400   10.0  24TX-lv11  3SX-8100  4.0.9    2.0

Average loopback load: 19.46% TX
(pkt size:60-1514 cycle:30 pkt/s:100 burst:1)

Connected port: 1a1

00:00:00 02:21:07 - Test started; Press 'q' to quit, '?' to display test parameters

Testing ports: 1a2-1a24 1b*
Dropped ports: none

Transmitted      400      Missing      0
Received         388      Out of order  0
In flight        12       Corrupt      0
Max in flight    24       Corrupt pktid 0
Hello           8        Bad length   0
Lcp message      0        Bad tag      0
Other            0        Send error   0
Packet rate      100 pps
Loopback load    19.46 %
Packet size      840

***** 00:00:04 02:21:11 - SLOT 1: mac 0 1 1: link
***** 00:00:04 02:21:11 - SLOT 1: 10Mbps HDX

Testing ports: 1a2-1a24 1b*
Dropped ports: none

Transmitted      1053     Missing      0
Received         465     Out of order  0
In flight        588     Corrupt      0
Max in flight    588     Corrupt pktid 0
Hello           15      Bad length   0
Lcp message      2       Bad tag      0
Other            0       Send error   0
Packet rate      99 pps
Loopback load    19.46 %
Packet size      542

Test packets timed-out
Validating step 1314
An attempt to pass a packet through 1a1-1a19-1b2 has failed

00:00:34 02:21:41 - ERROR: Broken path; discarding bad port: 1a19

```

8. Select, Copy Save and Forward a dc Test File Segment

Depending on the duration of the dc test, the test file may be very large. Use the following procedure to select, copy, save, and forward segments of the test file to FORE Systems.

1. Access the properties dialog box for the window you are using to display the dc test results.
2. Select the Options tab page and check the Quick Select check box.
3. Select the Layout tab page and set the height parameter to the maximum: 9999.
4. Execute the dc Test.
5. Select the first line of the dc test display.
6. Move your cursor to the last line of the test and Shift Click to select the entire test results display.
7. Right click to copy the selected area to the clipboard..
8. Open a file using WinWord or another word processing program, and enter Control V to copy the test results to a file.
9. Attach the dc test results file to a mail message and send the message to:

Support@fore.com

10.2.3 NT Troubleshooting Tools

Using the NT 4.0 facilities available on a network management station attached via an in-band connection to the switch, you can trace packets routed from the NSC to the switch and to other devices in the network.

You can also configure the NSC to log errors and view NSC log files on your management station.

1. Using the NT Event Viewer To View Events

Using the NT Event Viewer you can view the NSC's event log, where the NSC's NT operating system writes system events.

The Event Log

As shown in the following sample, NT writes three types of events to the event log:

- Information events - identified by a blue icon
- Cautionary events - identified by a yellow icon
- Error events - identified by a red icon

NSC Events

NT logs events that it receives from the NSC along with internal events in its Event Log. The Event Log provides information to identify the source of these events. The NSC writes events from two FORE Systems components to the Event Log:

- SCC
- SCCM

SCC Event Codes

SCC logs these event codes to indicate the following event types occurred:

- 1015-informational events
- 1015-cautionary events
- 1015-error events

SCCM Event Codes

The SCCM generates the following event codes, that correlate to the event types shown below:

<u>Event Type</u>	<u>Range</u>
Information	1000 – 3000
Error	8000 – 10000

2. Accessing the Event Log

You can open the NT Event Log using ESX-Cli or the NT Event Viewer

Open the Event Log using this ESX-Cli command:

```
show log <log name>
```

Where log name = **system**, **security**, or
application

Open the Event Log with Event Viewer by beginning at the Start Menu and following this command sequence:

Select Programs, Administrative Tools, Event Viewer

When Event Viewer starts up, pull down the Log menu and select system, security, or application,

To select the NSC whose log you want to view:

- Pull down the Log Menu and click the Select Compute menu item..
- Enter the NSC name in the Computer field to display the Event Log for that NSC

3. Viewing Event Detail Information

Select the event you want to view and double click to display more details on the event.

4. Reporting Events to Technical Support

When a halt occurs, examine the Event Log for error events then contact FORE Systems Technical Support and report the event source, the event code and the event text.

Note: To obtain detailed information for an event, including the event text, double click on the entry in the Event Log

10.3 Startup and Hardware Problems

This section describes problems that may occur during the startup sequence that affect the Network System Controller (NSC) and the Hardware Forwarding Engine (HFE).

<u>Problem</u>	<u>Section</u>
• NSC Startup	10.3.1
• HFE Startup	10.3.2
• Administration and Configuration	10.3.3
• User Equipment	10.3.4

10.3.1 NSC Startup Problems

Check the indicators located on the NSC that indicate normal operating status during startup.

<u>Check</u>	<u>Chapter</u>
• NSC has power	2 <i>ESX-4800</i> , 3 <i>ESX-2400</i>
• Disk drives have power	2 <i>ESX-4800</i> , 3 <i>ESX-2400</i>
• Fans have power	2 <i>ESX-4800</i> , 3 <i>ESX-2400</i>
• Adapter 1 card Link LED ON	2 <i>ESX-4800</i> , 3 <i>ESX-2400</i>

10.3.2 HFE Startup Problems

Check the indicators located on the HFE that indicate normal operating status during startup.

<u>Check</u>	<u>Chapter</u>
• HFE has power	2 <i>ESX-4800</i> , 3 <i>ESX-2400</i>
• Fans are operating normally	2 <i>ESX-4800</i> , 3 <i>ESX-2400</i>
• Port LEDs show normal status	4

10.3.3 Administration and Configuration Problems

In the event that startup does not complete normally, check the following:

<u>Check</u>	<u>Chapter</u>
• HFE-to-NSC cable connection	2 <i>ESX-4800</i> , 3 <i>ESX-2400</i>
• Switch management and control paths	4.2
• Management software installation	4.4
• Access to the chassis display	4.5

Note: As described in Section 4.5, when startup completes, normally, you will see the chassis view on your screen. To confirm that you are connected to the switch, you can execute this ESX-Cli command at the ESX-Cli prompt:

```
show chassis status
```

10.3.4 User Equipment Problems

In the event that you experience problems with user equipment during or following startup, check the following:

<u>Check</u>	<u>Chapter</u>
• HFE-to-user equipment cable connection	4.3
• Port LEDs	4.3

10.4 Ethernet Problems

This section describes Ethernet-related problems that may occur either during startup or while the switch is in an operational state.

<u>Problem</u>	<u>Section</u>
• Port Initialization	10.4.1
• Data Corruption	10.4.2
• CRC Errors	10.4.3
• Lost Frames	10.4.4
• Performance	10.4.5

10.4.1 Port Initialization Problems

Port initialization problems include the following.

- Auto-negotiation doesn't work
- Port won't come up
- Port is bouncing

To verify that ports are initialized, you can execute this ESX-Cli command at the ESX-Cli prompt:

```
show enet status port *
```

10.4.2 Data Corruption Problems

You can detect when data corruption errors occur, by executing this ESX-Cli command at the ESX-Cli prompt:

```
show enet errors port *
```

Using fault isolation techniques you can isolate the problem to a particular external device, a particular port, media, or line card.

10.4.3 CRC Problems

You can detect when CRC errors occur, by executing this ESX-Cli command at the ESX-Cli prompt:

```
show enet errors port *
```

10.4.4 Lost Frame Problems

You can detect when Lost Frames occur, by executing this ESX-Cli command at the ESX-Cli prompt:

```
show enet packets port *
```

10.5 Bridged Network Problems

This section describes Bridged Network problems that may occur when the switch is operating. For problem information refer to the following sections in the **Administrator's Guide**:

<u>Problem</u>	<u>Section</u>
• Connection	10.5.1
• Session	10.5.2
• Transmission	10.5.3
• Spanning Tree	10.5.4
• Looping and Broadcast storm	10.5.5

10.5.1 Connection Problems

Connection problems can prevent devices from communicating through the switch. In addition to the physical connection problems described in Section 10.4, Ethernet problems, you need to verify that the device's:

<u>Check</u>	<u>Chapter</u>
• MAC address is set correctly	6
• Port is assigned to the correct bridge group	6

10.5.2 Session Problems

Session problems can prevent a connection from being established between two devices attached to the same bridge group. You need to verify that both devices are attached to the same bridge. See *Chapter 6*.

10.5.3 Transmission Problems

You may encounter the following problems that affect the delivery of frames to the proper ports:

- Frames don't come out on the expected port

Suspects include:

- forwarding database entry incorrectly set
- spanning tree bouncing

- Frames come out the wrong port

Suspects include:

- duplicate MAC address
- unreconciled network loop
- forwarding database entry incorrectly set

- Frames come out on all ports

Suspects include:

- unknown destination address (DA) flooding
- forwarding database full
- multicast/broadcast set incorrectly

10.5.4 Spanning Tree Problems

If you encounter the following problems, check your Spanning Tree configuration—see Section 6.4.

Problem

- Bounce
- Designated bridge is incorrect
- Root bridge is incorrect
- Wrong port is in standby state

10.5.5 Looping and Broadcast Storms

Looping and broadcast storms can block the flow of packets within the bridge group. You can configure spanning tree to eliminate looping on the bridge group—see Section 6.4. To minimize broadcast storms, the network can be partitioned by routers into separate broadcast domains.

10.6 TCP/IP Problems

As a starting point for troubleshooting TCP/IP problems you may want to verify that the switch and network are properly configured. For configuration information refer to the following sections in the **ESX Switch Administrator's Guide**:

<u>Problem</u>	<u>Section</u>
• IP Addressing	7.7.1
• TCP/IP Networks	7.7.1
• OSPF Networks	7.7.2
• RIP Networks	7.7.3
• Static Routes	7.7.4
• DHCP	7.7.5

Note: When debugging IP problems for RIP and OSPF, you can set a parameter in the IP Configuration screen to Log the maximum amount of information.

10.7 SNMP Problems

When troubleshooting SNMP problems, you can perform the following checks to verify connectivity and compatibility between the switch and external network management applications—for example, HP OpenView.

Perform

- Ping
- Network connectivity
- Run Network Monitor

Verify

- IP connectivity
- Physical connectivity
- Queries are being sent

10.8 Managing Disks and Reconstructing Arrays

The NSC has two hard drives that are mirrored to provide backup for the ESX software and the configuration files that you save to disk.

Using the hot-swappable, two-hard-drive feature and the Adaptec software, you can replace a failed drive with a spare drive and reconstruct the disk array, if a disk failure occurs.

The following sections cover these topics related to managing disks and reconstructing disk arrays:

- Detect a drive failure in the log
- Start Adaptec and verify a drive failure
- Rescan the array
- Remove and replace a drive
- Reconstruct an array

10.8.1 Detect a Hard Drive Failure

When a single hard drive fails, the NSC will continue to run, without drive mirroring. The switch will continue to run while you hot-swap the failed drive with a replacement drive.

Caution: To avoid corrupting your source disk, only use drives that are labeled **SPARE** as replacements.

Although the Red LED on the drive *may* turn on when a failure occurs, the Adaptec CIO Array Management Software logs all disk management errors to the NSC's system event log.

Using the Event Viewer on your management station, you can access the NSC's system event log and scan it for indications of hard drive failures—see *illustration*.

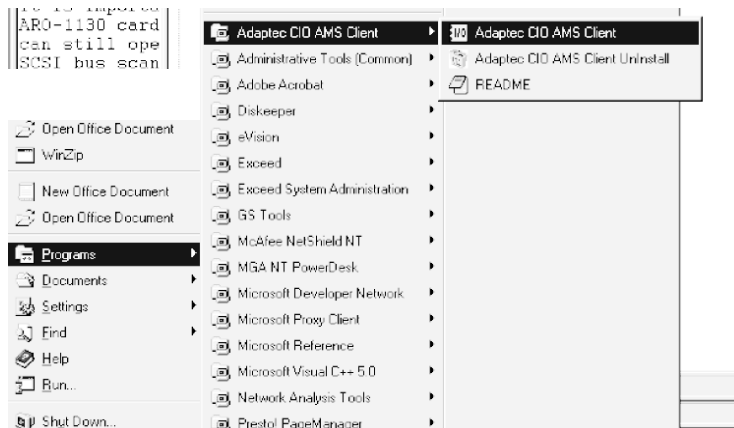
Log View Options Help						
Date	Time	Source	Category	Event	User	Computer
5/15/98	7:03:05 PM	CIOArrayManagem	None	1	N/A	nsc-mdl
5/15/98	7:03:05 PM	CIOArrayManagem	None	1	N/A	nsc-mdl
5/15/98	7:03:05 PM	CIOArrayManagem	None	1	N/A	nsc-mdl
5/15/98	7:03:02 PM	CIOArrayManagem	None	1	N/A	nsc-mdl
5/15/98	6:52:25 PM	CIOArrayManagem	None	1	N/A	nsc-mdl
5/15/98	6:52:25 PM	CIOArrayManagem	None	1	N/A	nsc-mdl
5/15/98	6:52:25 PM	CIOArrayManagem	None	1	N/A	nsc-mdl
5/15/98	6:47:48 PM	CIOArrayManagem	None	1	N/A	nsc-mdl
5/15/98	6:47:48 PM	CIOArrayManagem	None	1	N/A	nsc-mdl
5/15/98	6:41:40 PM	CIOArrayManagem	None	1	N/A	nsc-mdl
5/15/98	6:41:37 PM	CIOArrayManagem	None	1	N/A	nsc-mdl
5/15/98	6:41:37 PM	CIOArrayManagem	None	1	N/A	nsc-mdl
5/15/98	6:36:25 PM	CIOArrayManagem	None	1	N/A	nsc-mdl
5/15/98	6:36:25 PM	CIOArrayManagem	None	1	N/A	nsc-mdl
5/15/98	6:36:21 PM	CIOArrayManagem	None	1	N/A	nsc-mdl

10.8.2 Start Adaptec and Verify a Drive Failure

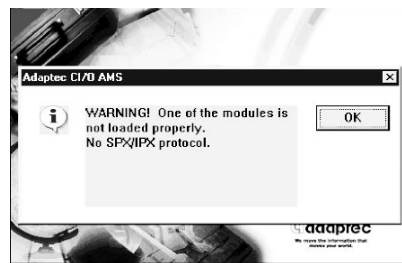
After noticing that you have a hard disk failure, *by checking the NSC's system log*, start the Adaptec C/IOArray Manager. You need to start the Array Manager in order to check the condition of the disk array.

To start the Adaptec Array Manager:

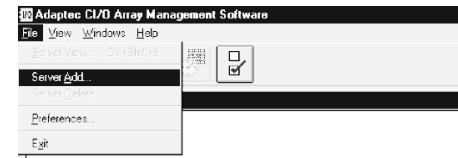
1. From the Start menu, select the Adaptec CIO AMS Client:



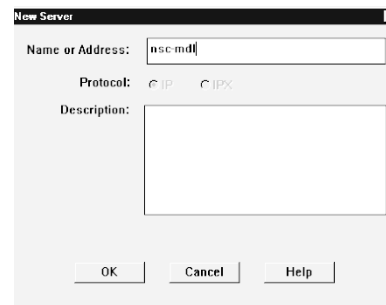
2. A warning message will appear. Click OK to display the main Adaptec Software screen.



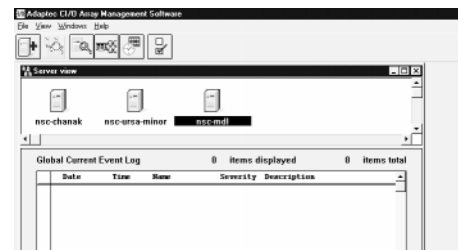
3. On the main Adaptec software screen, pull down the file menu and select Server Add.



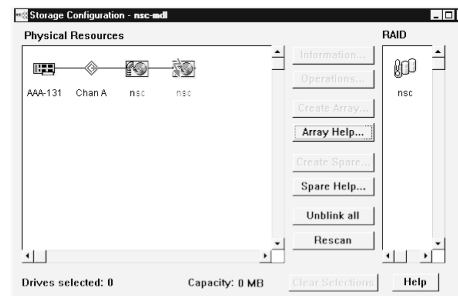
4. Type in the name of the NSC and click OK to return to the main menu.



4. On the main menu, click the NSC icon you added.



5. On the Storage Configuration dialog, notice that the NSC drive on the right has an arrow to indicate a bad hard disk.



10.8.3 Rescan a Disk Array

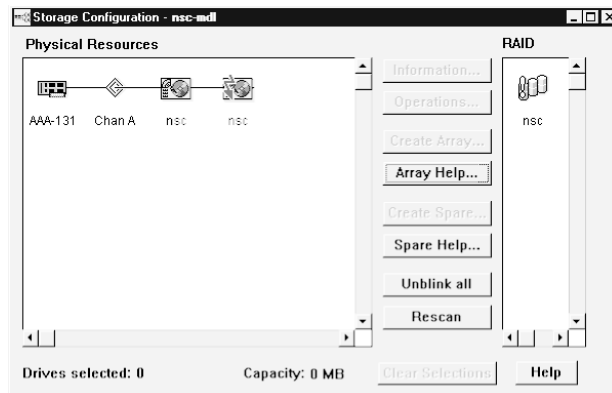
After determining that you have a hard disk failure with Adaptec, perform the following procedure to rescan the array.

If the rescan is successful the array will be restored to its former, intact state. If the rescan is unsuccessful, Adaptec will remove the broken drive from the display, leaving a single drive in operation.

Caution: To avoid corrupting your source disk, only perform a Rescan with the original, factory-installed drives or after inserting a replacement drive labeled **SPARE** and successfully reconstructing the array.

Perform these steps to Rescan an array:

1. From the storage configuration screen, click Rescan.



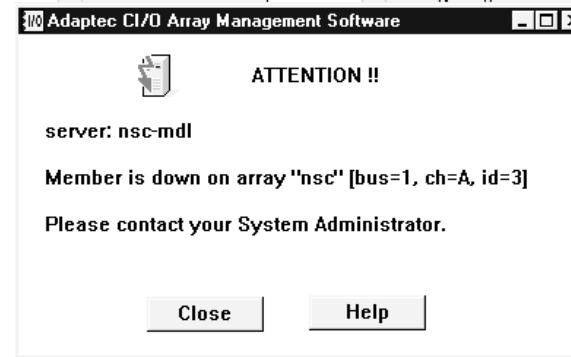
2. Click OK and enter your NSC password.



3. If the Rescan was successful, this screen will appear:



4. If the Rescan was unsuccessful, this screen will appear:



Continue with the next section to remove and replace the bad drive.

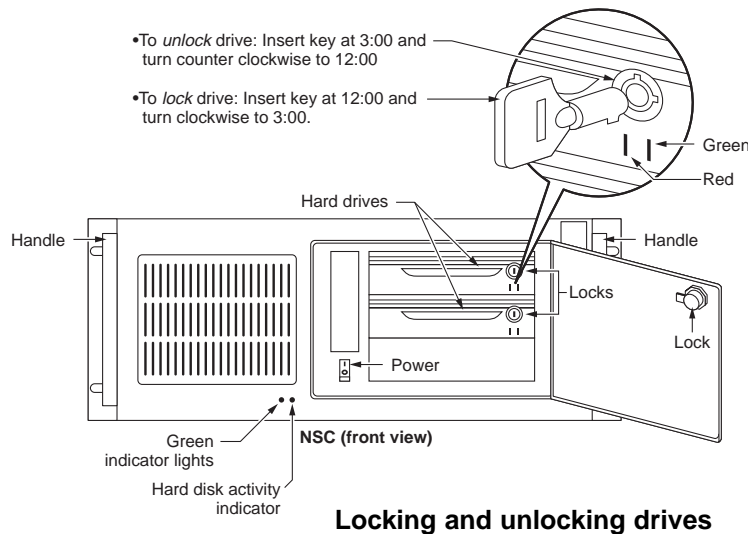
10.8.4 Remove and Replace a Drive

After determining you have a hard disk failure and identifying the bad drive using the Adaptec Array Management software, follow these procedures to remove and replace a bad drive.

Remove a failed drive

1. If the NSC's drive door is locked, use a key to open it.
2. Insert a key in the drive locking mechanism and unlock it—see *illustration detail*.
3. Remove the drive by pulling on the handle on the front of the drive and support the back of the drive as you slide it out of the drive bay.

Note: After you remove it, look at the back of the drive, and make note of its SCSI number (0 or 1).



Replace a failed drive

1. Locate a spare drive.
Caution: To avoid corrupting your source disk, only use drives that are labeled **SPARE** as replacements.
2. Set the SCSI number of a drive labeled **SPARE** to the same value (0 or 1) as the SCSI number of the drive you are replacing. If necessary, change its SCSI number by placing a screwdriver in the SCSI Adapter Indicator slot and turn the slot until it points to the correct number.
3. Remove the **SPARE** label attached to the replacement drive before you insert it in the drive bay.
4. Hold the handle of the drive and support it at the back as you slide it into the drive bay.
5. Insert a key in the drive locking mechanism and lock it—see *illustration detail*.
6. Lock the drive door on the NSC.

Continue with the next section to reconstruct the disk array.

10.8.5 Reconstruct an Array

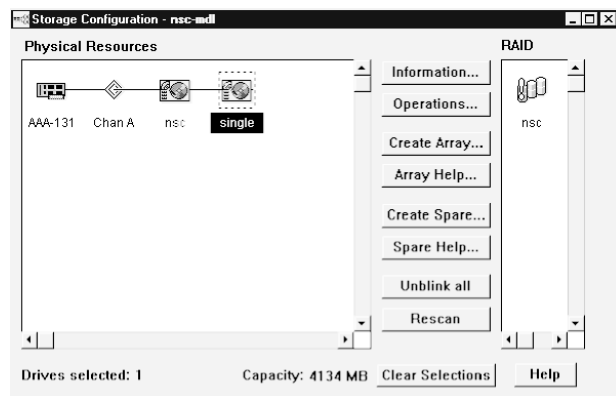
Follow this procedure to reconstruct the array after you have replaced a drive in the array with a spare drive. During this procedure, the Adaptec software will copy the contents of the NSC drive to the single drive and create a mirrored array.

In the previous section, when you inserted the replacement drive into the drive bay, the system checked both drives and displayed the drive marked **SPARE** as *single* in the Storage Configuration window—for example:

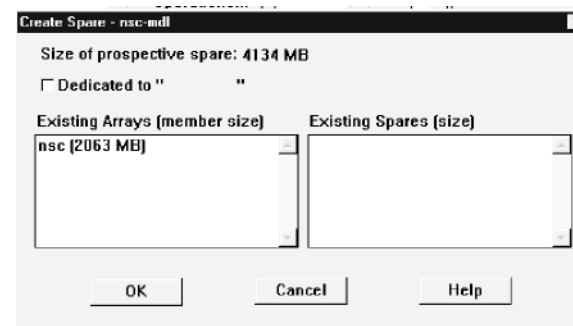


To reconstruct an array:

1. Click on the *single* icon and click the Create Spare button.



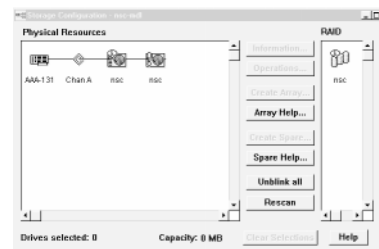
2. Click the OK button on the Create Spare dialog box.



3. Click OK on the Warning Dialog box and enter your password in the Password dialog box.



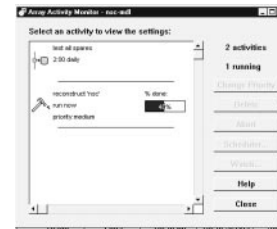
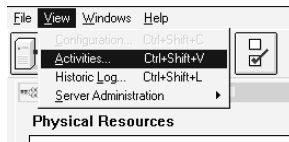
The icons will change on the main menu, indicating the array is under reconstruction.



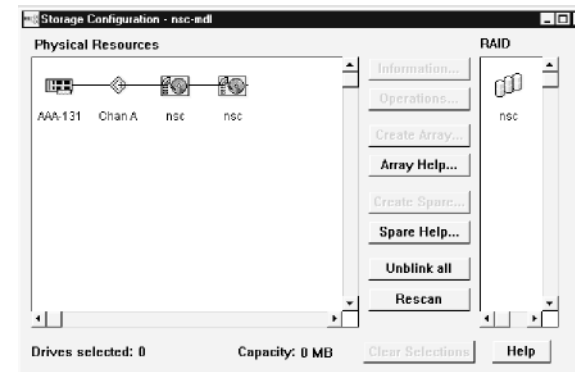
10.8.5 Reconstruct an Array (continued)

4. You can pull down the View menu, select Activity to launch the Activity Monitor, and then check the progress.

Note: It takes approximately ten minutes to reconstruct the array.



5. When the reconstruction completes successfully, the drive icons will both say NSC, and no arrows will be displayed over the NSC icons. Close the dialog box, and close the main Adaptec window to return to normal operation.



10.9 Reporting Problems

If you are unsuccessful in your attempt to troubleshoot switch and network problems, or if you determine that an uncorrectable hardware or software problem exists, follow the procedure outlined in your maintenance agreement to receive the necessary technical support.

Opening a Case with FORE Systems' Technical Support

If you have a support agreement with FORE Systems, we recommend that you open a case when you encounter a problem with your switch. By opening a case, you gain the immediate attention of FORE Systems' Technical Support and simplify problem communication, tracking, and resolution.

To open a case with Technical Support:

1. Access the FORE Systems website *www.fore.com*
2. Select Technical Support.
3. Follow the procedure on the Technical Support page to open a case.

In addition, we would like to hear from you directly. We will work with you closely to resolve any problems that you may encounter.

Technical Support

In the U.S.A., you can contact FORE Systems' Technical Support using any one of the following methods:

1. You can receive online support via TACtics Online at:
<http://www.fore.com/tac>
2. You can contact Technical Support via e-mail at:
support@fore.com
3. You can telephone your questions to Technical Support at:
1-800-671-FORE (3673) or +1 724-742-6999
4. You can FAX your questions to Technical Support at:
+1 724-742-7900

Technical support for non-U.S.A. customers should be handled through your local distributor.

No matter which method is used for support, please be prepared to provide:

- Your support contract ID number
- The serial number(s) of the product(s)
- As much information as possible describing your problem/question.

This chapter provides an overview of application policies. You can create a policy for an application and assign that policy to a particular port. When the switch checks the information in each packet it receives or sends, it will determine that a policy has been set and take the action the policy requires it to take.

This chapter describes how to create and configure new policies, how to add and remove ports from existing policies and how to view policy summary information:

- 11.1 Policies Overview
- 11.2 Policies and How They Work
- 11.3 Creating Application Policies
- 11.4 Adding Ports to a Policy
- 11.5 Removing Ports from a Policy
- 11.6 Deleting an Application Policy

11.1 Policies Overview

Policies provide a means of using the switch itself to control the flow of traffic through the switch at wire-speed, as it receives and forwards each packet.

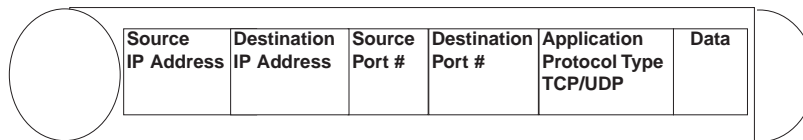
You set application policies using ESX-Admin to:

- Name the policy
- Associate an application with the policy
- Specify a port where the policy will be applied
- Specify an action to take

When you set a policy, the switch examines the header of every packet to determine if the policy should be applied. Then it takes the action you specified on that packet.

11.1.1 The Packet Header

Prepended to the data contained in the packet, the packet header contains two essential pieces of information that the switch uses to determine whether to enforce a policy: the source and destination IP addresses and the source and destination port numbers.



11.1.2 Source and Destination IP Addresses

The source and destination IP addresses in the packet identify the inbound and outbound *physical ports* on the switch. The switch learns the port where the packet arrived and the port where it will forward the packet by looking up information it maintains that associates physical ports with IP addresses.

11.1.3 Source and Destination Port Numbers

The source and destination port numbers in the packet identify the client and server TCP or UDP port that sent or that will receive the data in the packet.

This port number information is also called the *application port number*. Each application has a unique application port number or set of port numbers that identify the application as the packet moves up and down the TCP/IP stack. IANA maintains a list of standard application port numbers.

11.1.4 Determining Whether to Enforce a Policy

To determine whether to enforce a policy on a packet, the switch uses information in the:

- Application policy—to determine which application policy is in force and the action to take on that packet.
- Source and destination IP addresses—to determine if the port has a policy in force.
- Source and destination application port numbers—to determine which application is sending or receiving the packet.
- Application protocol type—to determine which protocol the application is using—TCP or UDP.

11.1.5 Policy Actions

The application policies that you configure direct the switch to take action on a packet. Once it determines that a policy should be enforced, the switch performs one of the following actions:

- Sets the packet priority—high medium or low
- Drops or redirects the packet to another port

11.2 Policies and How They Work

Policies specify the actions a switch will take when it determines a certain condition or set of conditions exists. By creating application policies, you can control the flow of packets through the switch. Policies can be global or specific, depending on where you apply the policy in the network.

11.2.1 Creating and Enforcing Policies

When you create a policy, you not only assign the policy to an application, you also assign the policy to a particular port or group of ports. When the ESX switch processes a packet, it looks for the application identifier in the packet and checks the physical port number where the packet is being received or sent. If a policy exists for that application on that port, it executes the action the policy defines on that packet.

11.2.2 Actions

When you create a policy, you define an action that you want the ESX switch to take when it encounters traffic that is sent by or will be received by a specific application. The switch can take one of the following actions on traffic generated by an application; it can:

- Raise or lower the priority of that application's traffic—relative to traffic from other applications.
- Drop that application's traffic.
- Redirect that application's traffic to a specific switch port.

Note: You can redirect traffic to a specific port on the switch—for example, to a port where a network analyzer is attached.

11.2.3 Policies and Application Port Numbers

A policy instructs a switch to take a certain action when it encounters a packet from a specific application. Each packet contains an application identifier or port number. A switch reads the port number in a packet to identify the application.

IANA maintains the list of standard application port numbers that are consistently used in all networks. For example, FTP port numbers are 20 and 21. Port numbers fall into three categories:

- Well-known
- Registered
- Private or dynamically-assigned

Note: Use IANA specified port numbers when you define port numbers for your applications. Assign a port number in the range of private or dynamically-assigned numbers to applications that are not well-known or registered.

11.2.4 Global and Specific Policies

Using ESX-Admin, you can only set policies for the switch to which you are connected. Policies that apply only to a particular switch are called *specific policies*. Policies that apply to more than one node on the network are called *global policies*. To set global policies, you must use the Directory Console. See the **FORE Systems Directory Enabled Networking Guide** for details on setting global policies.

Note: You can view all the policies that apply to the switch to which you are connected by selecting the Policies icon displayed in the Tree View and checking the policies information that is displayed in the tree view.

11.3 Creating an Application Policy

To create an application policy, you need to configure it by accessing the Application Policy page and specifying the following information:

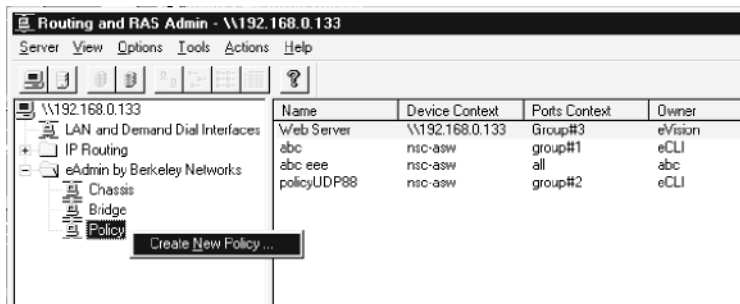
- Name the policy.
- Specify the ports to which the policy will apply.
- Set the parameters for the application.
- Specify the action the switch will perform

11.3.1 Access the Application Policy Page

You can access the Application Policy page from either the Tree View or the Display View.

In Tree View:

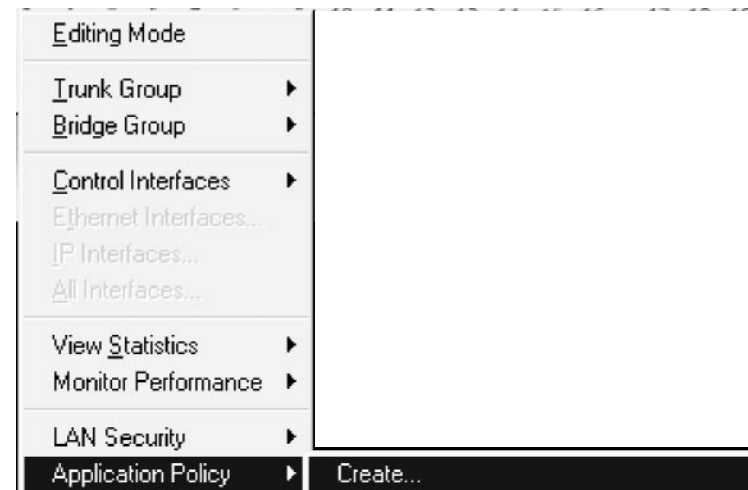
1. Select the Policy icon.
2. Right click to display the Create New Policy...popup.
3. Click the Create New Policy...popup to display the Application Policy page.



OR

In Chassis View:

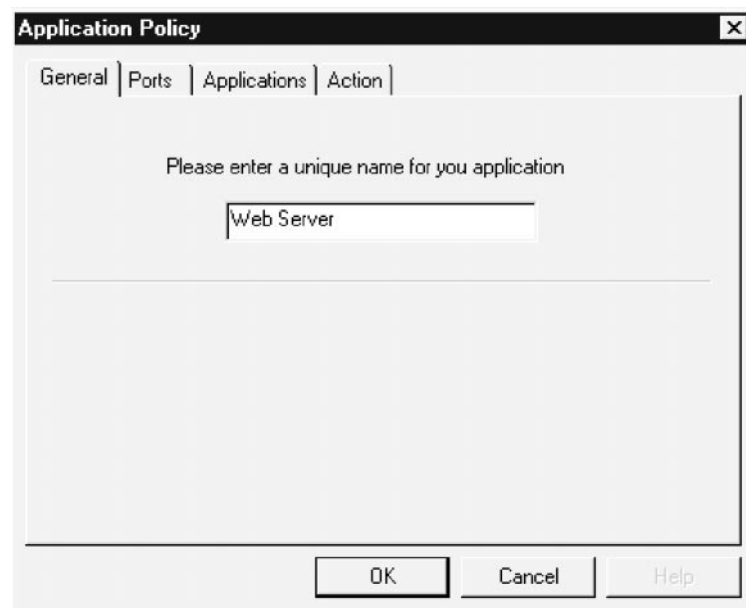
1. Select a port.
2. Right click to display the Edit Menu and select Editing Mode.
3. Right click to display the Edit Menu again.
4. Select Application Policy to display a popup, then select Create to display the Application Policy page.



11.3.2 Name the Application Policy

To name the application policy:

1. Enter the name of the policy in the policy window.
2. To continue, click the Ports tab.



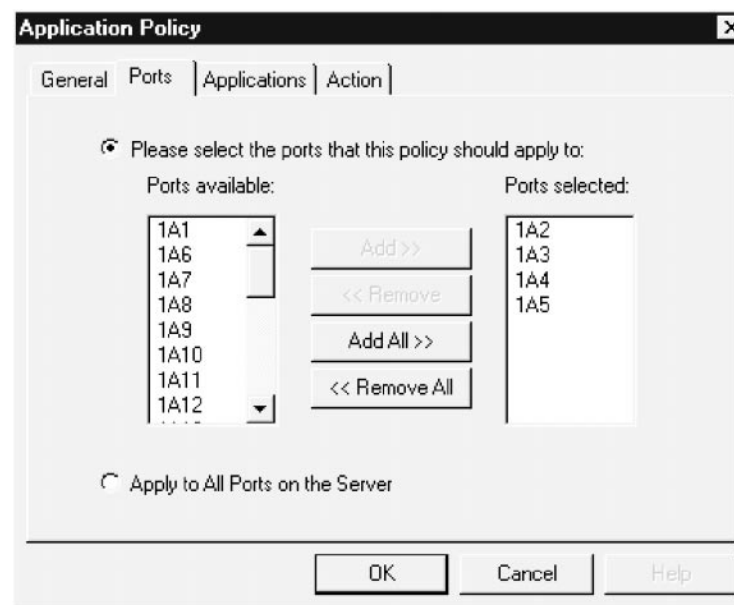
11.3.3 Select the Ports for the Policy

To define the ports to which the policy will apply:

1. Either double-click on a port in the ports available window
OR
Select a port or group of ports and click the Add button
OR
Click the Apply to All Ports on the Server radio button

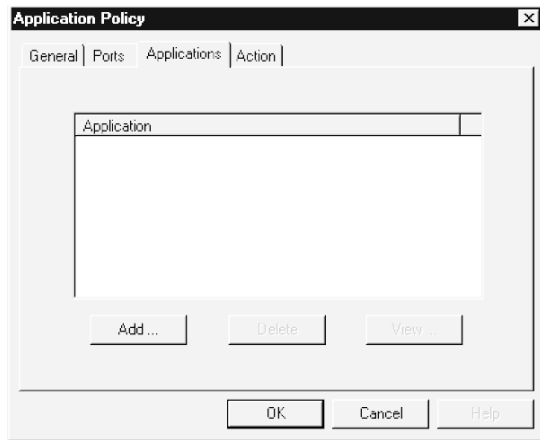
Note: The ports you select will move to the Ports selected window.

2. To continue, click the Applications tab.

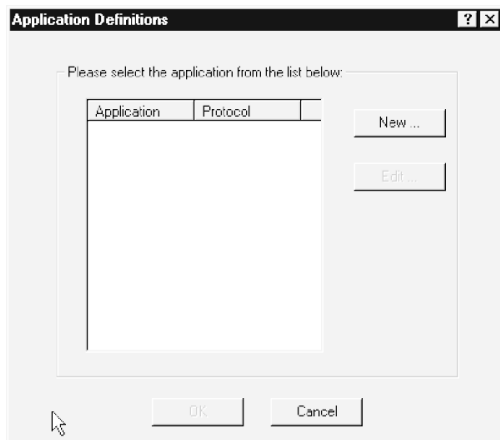


11.3.4 Add an Application to the Policy

1. Select the Applications Tab and click the Add button

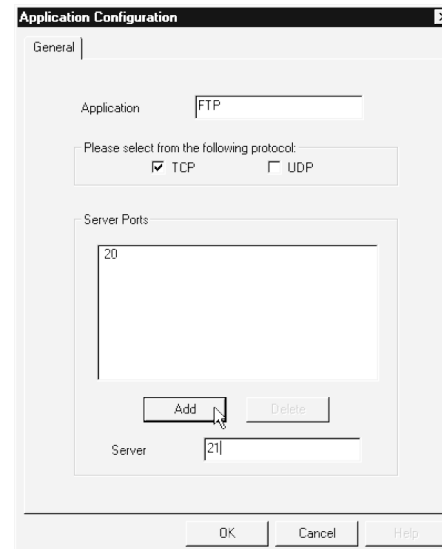


to display the Application Definitions page.



2. Click the Add button to display the Application Configuration page.

3. Enter the Application name in the Application text window.



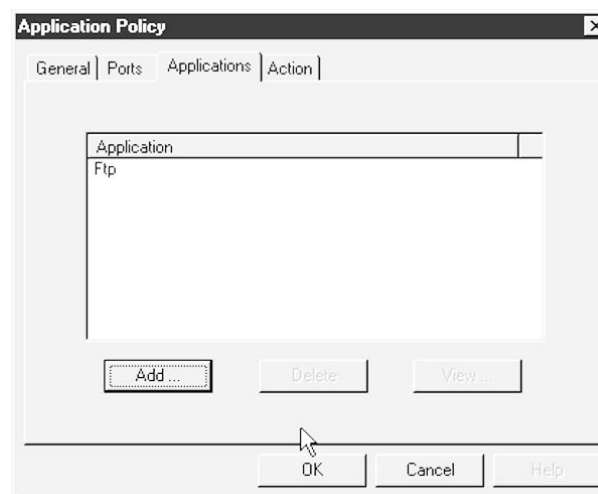
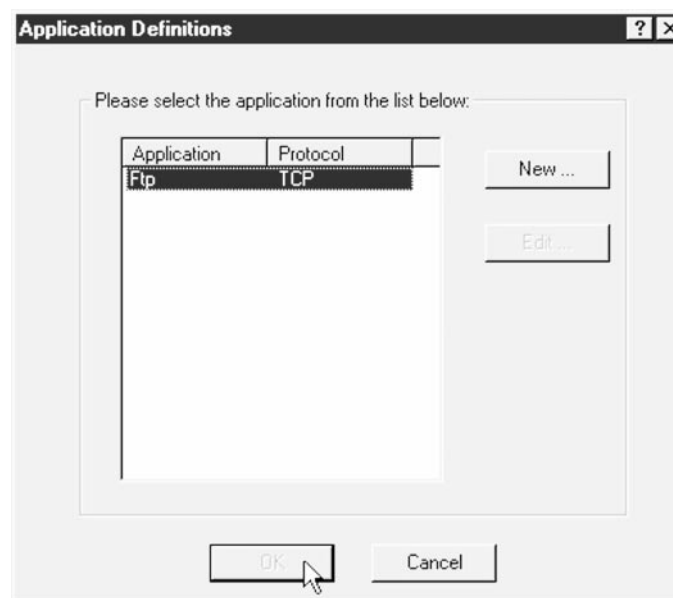
4. Enter an application port number in the Server window and click the Add button.

Note: Repeat this step for applications that have multiple port numbers, *for example-FTP*.

5. Click the OK button to redisplay the Applications Definition page.

11.3.4 Add an Application to the Policy (continued)

1. Select the Application you want to add to the policy and click the OK button to display the Application Policy page.
2. Click the Add button to display the Applications Tab page.
3. Select the application, and click the Add button.
4. To continue, click the Action Tab.



11.3 Creating an Application Policy

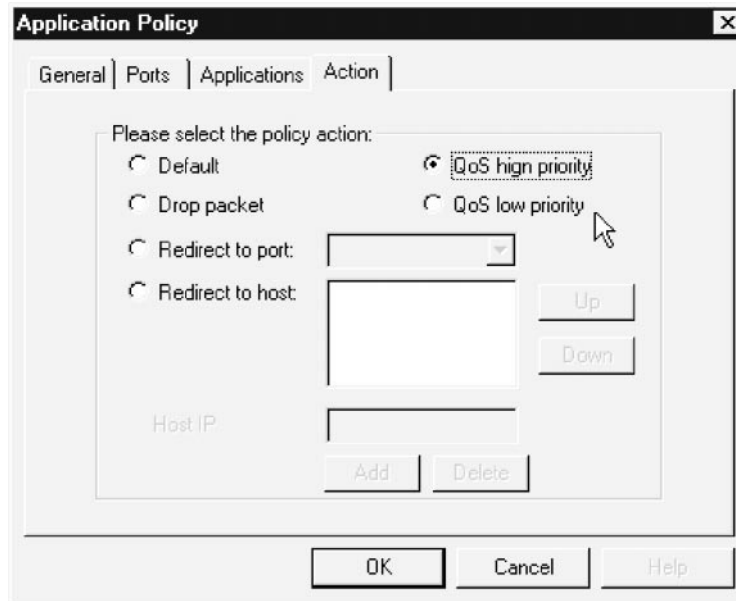
Chapter 11 Configuring Policies

11.3.5 Specify the Policy Action

1. Click a radio button to specify an action you want the policy to perform when it detects a packet coming from/going to the application you have specified.

Note: If you specify the redirect to host option, you will need to type the host IP address in the Host IP window and click Add. For the Redirect to host option to work, the host must be directly connected. To provide redundant redirection, you can specify multiple host IP addresses.

2. Click OK to complete the definition of the Application policy.

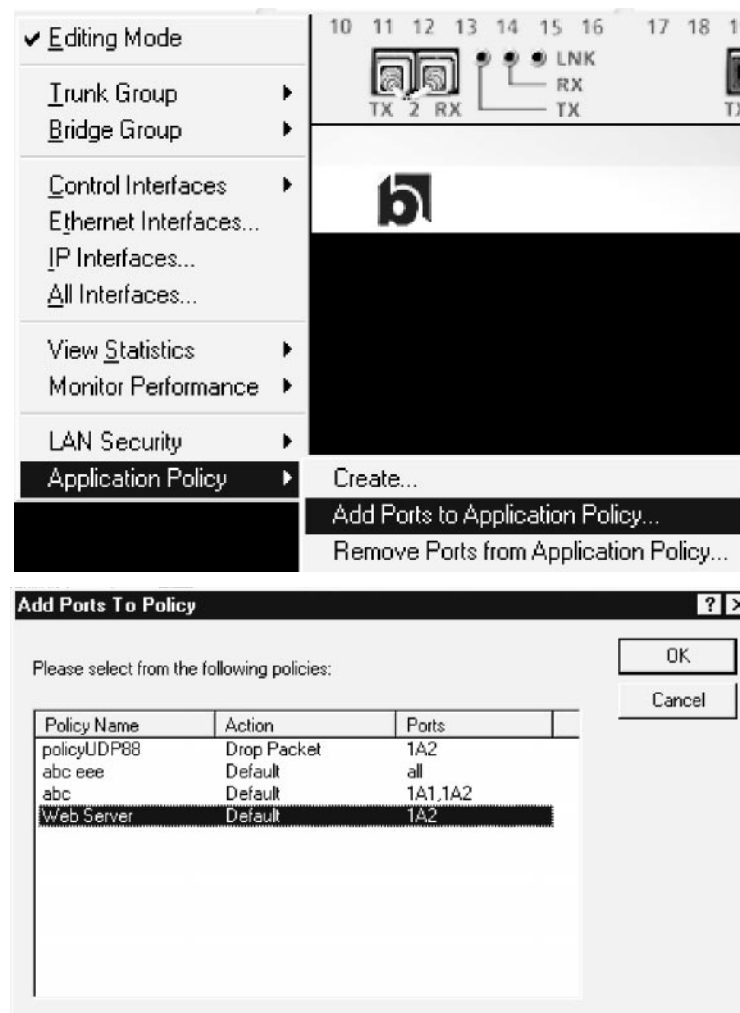


<u>Selection:</u>	<u>Description</u>
Default	Use the default QoS priority that you established at a global level when sending the packet.
Drop Packet	Do not forward the packet.
QoS Hi Priority	When sending the packet, assign it a high priority.
QoS Lo Priority	When sending the packet, assign it a low priority.
Redirect to Port	Forward the packet to the specified port, instead of sending it to the port specified in the packet.
Redirect to Host	Redirects the packet to the host whose IP address is specified. Note: For the Redirect to host option to work, a host must be directly connected.

11.4 Adding Ports to a Policy

After you define an application policy, you can add additional ports to the policy by following this procedure:

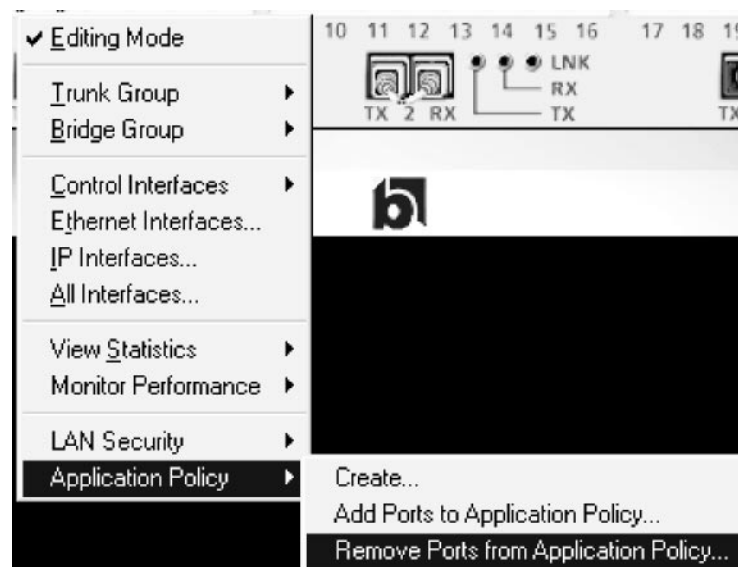
1. Select a port or group of ports.
2. Right click to display the Edit Menu and select Editing Mode.
3. Right click to display the Edit Menu again.
4. Mouse over Application Policy to display a popup, then mouse over Add Ports to Application Policy and release the mouse button to display Add Ports to Policy page.
5. On the Add Ports to Policy page, select the policy you want to apply to the port or group of ports you selected.



11.5 Removing Ports from a Policy

After you define an application policy, you can remove ports from a policy by following this procedure:

1. Select a port or group of ports.
2. Right click to display the Edit Menu and select Editing Mode.
3. Right click to display the Edit Menu again.
4. Mouse over Application Policy to display a popup, then mouse over Remove Ports from Application Policy and release the mouse button to display Remove Ports from Policy page.



11.6 Deleting an Application Policy

Follow this procedure to delete an application policy.

1. In Tree View, Select the Policy icon.
2. In Display View, select the policy you want to delete..
3. Right-click to display a popup menu, and select Remove to delete the application policy you selected in Step 2.

